PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:
H04L 9/00	A2	WO 00/01108
		(43) International Publication Date: 6 January 2000 (06.01.00)

(21) International Application Number: PCT/US99/13908

(22) International Filing Date: 21 June 1999 (21.06.99)

(30) Priority Data:
09/107,762 30 June 1998 (30.06.98) US

(71) Applicant: PRIVADA, INC. [US/US]; Two North First Street, San Jose, CA 95113 (US).

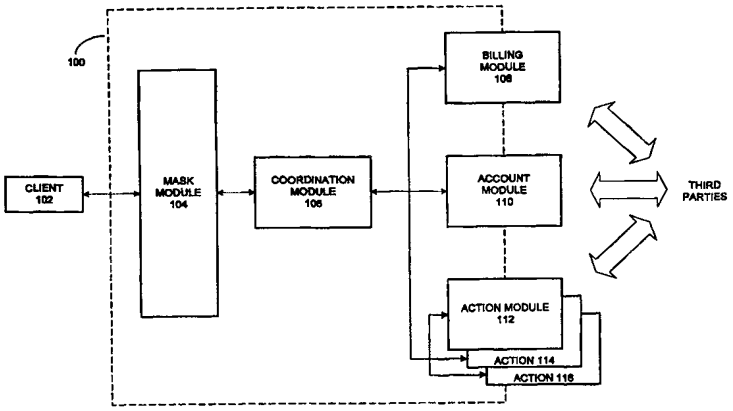
(72) Inventor: MCLAUGHLIN, Craig, Peter; 7448 Brighton Court, Dublin, CA 94568 (US).

(74) Agents: VAUGHAN, Daniel, E. et al.; Park & Vaughan, Suite 5, 399 Sherman Avenue, Palo Alto, CA 94306 (US).

(81) Designated States: CA, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: BI–DIRECTIONAL, ANONYMOUS ELECTRONIC TRANSACTIONS



(57) Abstract

A system and methods are provided provided for processing bi–directional, anonymous or pseudo–anonymous user transactions, including electronic mail and electronic commerce. A first digital certificate is used to authenticate a user when he or she connects to the system to conduct a transaction. A second digital certificate is created to authenticate the user's anonymous or pseudo–anonymous identity to third parties. The correspondence between the user's confidential identity (e.g., name, address, financial data) and true identity is unknown within the system during its normal operation. In normal operation a user connects to the system via a client module. The user's confidential identity is masked from a coordination module of the system, which coordination module coordinates tasks necessary to conduct the user's transaction or process the user's communication. A plurality of operating modules are provided to perform tasks such as billing, account management, sending or receiving electronic mail, conducting electronic commerce, etc. In normal operation, no module within the system possesses enough information to determine the user's confidential identity and connect the user to a particular transaction or a particular anonymous or pseudo–anonymous identity. In a monitor mode of operation, however, the content of transactions and communications processed for a particular anonymous or pseudo–anonymous user are recorded or logged pursuant to legal authorization or demand.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

BI-DIRECTIONAL, ANONYMOUS ELECTRONIC TRANSACTIONS

Field of the Invention

The present invention relates to the field of computer systems. In particular, a system and methods are provided for processing bi-directional, anonymous transactions in such a manner as to protect a user's confidential identity.

Background of the Invention

As computer systems become increasingly interconnected, the number of electronic transactions between distributed users grows commensurately. Electronic mail remains one of the most common types of transaction conducted between users, but other transactions are proliferating as well. In particular, electronic commerce has increased as methods of providing secure transactions have been developed.

Cryptographic security schemes that employ symmetric keys, such as Digital Encryption Standard (DES), are sometimes used to protect electronic communications, including electronic mail. With symmetric keys, the same key used to encrypt a message is used to decrypt it as well. Public key encryption (PKE) security schemes, such as RSA (named for its inventors: Rivest, Shamir and Adleman) by RSA Security, Inc., have also been developed. PKE schemes employ asymmetric key pairs wherein information encrypted with one key is decrypted with its complement. With PKE, communications between one entity and one or more other entities are secured by keeping one key "private" (i.e., known only to the single entity) while making the complementary key "public" (e.g., distributed among the other entities).

In addition to providing adequate security regarding the content and details of electronic transactions, there are a number of other features that are desired in systems for processing such transactions. Desirable features include authenticating a party's identity (i.e., ensuring that the party is who he or she claims to be), preventing repudiation of the transaction (i.e., preventing a party from disavowing his or her participation) and ensuring the integrity of the transaction (e.g., ensuring that a party can determine if the details or content have been altered).

In addition, demand is growing for the ability to transmit electronic communications and conduct electronic transactions in which one or more of the involved parties are anonymous or pseudo-anonymous.

Previous attempts to create a suitable environment for conducting electronic transactions have been unsuccessful in providing all of these features. In particular, those systems attempting to provide some form of anonymity have generally sacrificed some level of non-repudiation, authentication, or validity. In general, known systems provide less than satisfactory anonymity for users' confidential information or identities (e.g., name, address, financial data). For example, Pretty Good Privacy (PGP), a known scheme for protecting message contents, offers a fairly high level of authentication, validity, and non-repudiation, but provides no anonymity. An Internet service known by the Uniform Resource Locator (URL) of http://www.anonymizer.com provides anonymity between users and web sites, but the service remains aware of the users' confidential identities, thus falling short of true anonymity. In addition, this service is capable of providing anonymous electronic mail in only one direction (i.e., from users employing the service).

One system that provides a modicum of non-repudiation and anonymity is provided by DigiCash, Inc. Both parties involved in a DigiCash transaction (e.g., a merchant system and a consumer system), however, must be specifically configured to support the transaction protocol. Illustratively, the consumer system purchases DigiCash and tenders it to a merchant system. The merchant system must then trade it for more traditional currency. The DigiCash system does not, therefore, make existing forms of payment (e.g., credit cards) anonymous on either end of a transaction.

In addition, electronic transaction systems such as those described above are tailored to individual types of transactions (e.g., sending electronic mail, disbursing digital currency, submitting a news posting). A system providing the identified features bi-directionally (e.g., to and from an anonymous user) in a generally applicable system (i.e., multiple types of electronic transactions) is unknown.

Thus, there exists in the art a need for a system for securely conducting an electronic transaction or engaging in electronic communication while providing anonymity or pseudo-anonymity for a user's confidential identity. In such a system, a user is (pseudo-)anonymous not only to third parties, but to the system as well. In addition, such a system preferably makes the user anonymous or pseudo-anonymous regardless of the direction of the communication or

transaction (i.e., from or to the user). There also exists a need for method of operating such a system to perform multiple types of electronic transactions.

SUMMARY

In an exemplary embodiment of the invention, a system and methods are provided for exchanging bi-directional, pseudo-anonymous communications between a user and a third party. In this embodiment, the user is given pseudo-anonymity in order to mask his or her selected confidential identity (e.g., the user's true name, address or financial data), which confidential identity would otherwise identify the user in some manner. A pseudonym is provided for use in place of the confidential identity, such that transactions are performed for the user under cover of the pseudonym.

Thus, in this embodiment of the invention a communication directed from the user to a third party is received at an electronic intermediary. The electronic intermediary also receives a digital certificate from the user and authenticates the user by cryptographically verifying the certificate.

The pseudo-anonymous communication is then cryptographically signed with an asymmetric key associated with the user's pseudonym and the signed communication is transmitted to the third party. Although the third party is prevented from learning the user's confidential identity from the communication, the third party can authenticate the pseudonym using a cryptographic method.

In another embodiment of the invention, a pseudo-anonymous account is created on the intermediary for the user before he or she can conduct pseudo-anonymous transactions. In this embodiment, the user's true identity (e.g., the confidential identity that is masked by the user's pseudonym) is verified. Then, a second digital certificate, including a digital certificate of the intermediary, is generated and associated with the pseudonym. This second digital certificate is used by third parties to cryptographically verify the user's pseudonym after receiving a communication in the name of the pseudonym.

These and other embodiments of the invention will be described in greater detail with respect to the figures and description below.

DESCRIPTION OF THE FIGURES

FIG. 1 is a block diagram depicting a system for bi-directional, anonymous electronic transactions in accordance with one embodiment of the present invention.

FIG. 2 is a flow chart demonstrating a method of registering a new anonymous user account in accordance with an embodiment of the present invention.

FIGs. 3A-3B are flow charts depicting a method of establishing an anonymous user session in accordance with an embodiment of the present invention.

FIGs. 4A-4C are flow charts depicting a method of sending an electronic mail message from an anonymous user in accordance with an embodiment of the present invention.

FIG. 5 is a flow chart depicting a method of receiving a message for an anonymous user in accordance with an embodiment of the present invention.

FIG. 6 is a flow chart depicting a method of retrieving an anonymous user's electronic mail messages in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

The following description is presented to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

For example, although one embodiment of the invention described below provides a user with "name anonymity" wherein the protected confidential identity is the user's true name, the present invention is not limited to protecting a particular form of confidential identity. Other confidential identities may also be protected, such as the user's address, financial data (e.g., credit card number, bank account number) and the like. A user's pseudonym serves to protect whichever confidential identity she specifies.

A user's pseudonym may also correspond to various types of information. In one embodiment of the invention, a fictitious or otherwise false name, generated randomly or arbitrarily, is employed as a user's pseudonym. Other possibilities include the user's address or

electronic mail address. In addition, when the confidential identity to be protected comprises information other than the user's true name, his or her true name may be used as the pseudonym. One of ordinary skill in the art will thus recognize that a user's pseudonym may constitute virtually any information, other than the confidential identity of the user, and that the confidential identity that is protected need not be the user's true name.

Thus, in alternative embodiments of the invention various types of anonymity or pseudo-anonymity are provided, an illustrative sampling of which follows. When "address anonymity" is desired, a user's street address is protected by using, for example, her true name as her pseudonym. When a user requires "financial anonymity" (or "billing anonymity"), her credit card number or other confidential financial identity is secured by applying her true name or address as her pseudonym. In "physical anonymity," a user's physical mailing address can be masked with her email address. With "total anonymity," multiple confidential identities of a user (e.g., true name, true address, financial data) are screened by a pseudonym that is random or arbitrary.

Due to the various types of anonymity or pseudo-anonymity provided for a user in the myriad possible embodiments of the present invention, the terms "anonymous" and "anonymity" as they appear below should be understood to be interchangeable with "pseudo-anonymous" and "pseudo-anonymity." More generally, pseudo-anonymity should be understood to cover a range of degrees of anonymity, from minimally anonymous to truly anonymous.

Description of One Embodiment of the Invention

FIG. 1 depicts one embodiment of the invention in which a system and method are provided for bi-directional electronic communications conducted on behalf of a pseudo-anonymous party. System 100 allows a user to conduct electronic communications (e.g., electronic mail, commerce, banking, electronic transactions, and orders for physical transactions, goods or services) with third parties without the third parties learning a confidential identity (e.g., name, street or physical address, electronic mail address, IP address, financial identifier) of the user. A user is provided with a pseudo-anonymous identity, such as a pseudonym, to mask his or her confidential identity. Illustratively, a pseudonym takes the form of a non-confidential, but limited, identity of the user (e.g., where a user's confidential identity comprises his address, his pseudonym illustratively comprises his name).

Alternatively, however, a user's pseudonym comprises a random or arbitrary name, number or other alphanumeric sequence.

In normal operation of system 100 the user's confidential identity is unknown even within the system. However, as described below, should the user's transactions or other communications become subject to review or monitoring by a legally authorized entity (e.g., in response to a court order), the user's activities are processed in a "monitor" mode of operation in which the user's communications are captured or recorded. Illustratively, however, the user's activities performed prior to or subsequent to the period of monitoring are not compromised or revealed. In a present embodiment of the invention, during the monitor mode of operation the cryptographic keys employed to secure the user's communications are not revealed even though the contents of the communications are made available to the authorized entity.

With reference now to FIG. 1, system 100 is configured to provide anonymity to a user whose confidential identity comprises his name and whose pseudonym comprises an arbitrary or random name (e.g., Anonymous123). Those skilled in the art will, however, appreciate that virtually any other combination of pseudonym and confidential identity could be used. The user employs client 102 to access system 100. Client 102 is illustratively a web browser, a browser plug-in, a Java applet, an application patch, or a software program. Client 102 may be provided by the operator of system 100. Client 102 operates on the user's behalf in transactions processed by system 100. As discussed below, during a normal mode of operation of the illustrated embodiment, client 102 is the only element that is aware of both the user's pseudo-anonymous and confidential identities. In a "monitor" mode of operation (discussed in a subsequent section below), however, the confidential identity is stored in a secure form on system 100.

Mask module 104 is an interface between system 100 and client 102 in the illustrated embodiment of the invention. Mask module 104 masks characteristics of the user's confidential identity from third parties and the remainder of system 100. Although mask module 104 may learn the IP address of client 102, it does not have access to the user's pseudonym or the content of the user's transactions. As discussed below, mask module 104 generates a unique session identifier each time a user connects to system 100 to conduct a transaction. Illustratively, the session identifier is used to identify a particular user's communications with and/or within system 100 in place of information that may compromise

the user's anonymity. Thus, in the illustrated embodiment of the invention, the unique session identifier is used by mask module 104 and one or more other components of system 100 to identify a user's session while maintaining the user's anonymity.

Coordination module 106 coordinates the processing of anonymous communications through and within system 100. In particular, coordination module 106 manages a user's anonymous communications by coordinating and submitting relevant portions of each communication to one or more operating modules (e.g., billing module 108, account module 110 and action modules 112, 114, 116). Coordination module 106 helps ensure that each operating module is able to perform its portion of a user's transaction while remaining ignorant of other details of the transaction. Illustratively, each operating module receives from coordination module 106 only the information necessary to perform its portion of the user's transaction. As discussed in a subsequent section, in the "monitor" mode of operation coordination module 106 records or logs information concerning the content of transactions conducted by a monitored user. In a normal mode of operation, however, the details of anonymous transactions are unavailable to coordination module 106.

As discussed above, to protect a user's anonymity within system 100, a unique session identifier is used to identify each user session. In the illustrated embodiment, however, a unique identifier generated by mask module 104 is, within system 100, only used for communications between mask module 104 and coordination module 106. In this embodiment, coordination module 106 generates separate, unique, identifiers for each communication it passes to an operating module, and vice versa. Thus, every communication exchanged between the coordination module and an operating module has a different identifier (illustratively generated by the sender). One of ordinary skill in the art will recognize that by associating different identifiers with different portions of a user's communication or transaction it becomes more difficult to associate any one communication or transaction with a particular user. It also becomes more difficult for an intruder to piece together the myriad pieces of one communication or transaction.

System 100 interfaces with third parties through the operating modules in order to perform transactions and other communications on behalf of anonymous users, using their pseudonyms. Third parties include recipients and/or initiators of communications involving a user served by system 100. Illustrative third parties thus include, but are not limited to, electronic mail correspondents, billing parties, financial entities and electronic entities (e.g.,

web servers, Internet application servers). For purposes of the present invention, "communication" is understood to broadly encompass numerous types of information and data, regardless of form (e.g., graphical, numerical, audio) or method of encoding, and "transaction" is understood to include any transaction facilitated by such communication.

Billing module 108 illustratively performs activities necessary to bill the user for his or her activity, and thus connects to third party billing authorities (e.g., credit card issuers, digital cash authorities, value acquirers).

Account module 110 maintains account information for users based upon their pseudonyms (i.e., their pseudo-anonymous identities). Account information maintained on account module 110 includes the actions or types of transactions a user is authorized to conduct using system 100. Different types of accounts are created for different users based upon the transactions they wish to conduct; the type of account illustratively determines the permitted functions. Also, an indicator is stored with each user account to reflect whether the associated user is to be monitored (via the "monitor" mode of operation described in detail in the following section). In addition, account module 110 may act as an enhanced Certificate Authority (CA) for system 100. In its role as CA in one embodiment of the invention, account module 110 generates two digital certificates for each user, as discussed below.

Finally, system 100 may include one or more action modules among its operating modules. In an exemplary embodiment of the invention, action modules interface with third parties to deliver or exchange information or to perform operations on behalf of pseudo-anonymous users (e.g., by employing the user's pseudonym in place of his or her confidential identity). Illustrative services or functions offered by action modules include, without limitation: sending electronic mail, receiving electronic mail, browsing web sites and pages, posting news messages, conducting electronic commerce, participating in an Internet conversation (e.g., "chatting"), etc. Each action module is thus configured according to a specified function or role. For example, an electronic commerce action module must be conversant in commerce protocols while electronic mail action modules must understand various mail protocols. The functions and characteristics of exemplary action modules are well-known to those skilled in the art and need not be described in detail here.

The scope of the present invention is not limited to a particular quantity of action (or other operating) modules, or to particular functions performed by the various modules. Illustratively, however, each operating module receives only the information necessary to

perform its function and the information passed between the user and each operating module is encrypted and is thus inaccessible to either mask module 104 or coordination module 106 (except in the monitor mode of operation). For security purposes, then, in system 100 every module could maintain a memory area that is inaccessible to the other modules. Each module's memory illustratively comprises solid-state memory devices. In an embodiment in which the modules share a large memory device, software means are employed to prevent access to other modules' memory areas. In alternative embodiments of the invention, the modules' memory includes software constructs (e.g., data structures such as arrays, heaps, queues), electronic storage media (e.g., magnetic disk, optical disk, tape, compact disc), and still other memory elements known to those skilled in the art.

FIG. 1 depicts an embodiment of the invention in which each module (i.e., client, mask, coordination, billing, account and action modules) is nominally separated from each other. This nominal separation amounts to geographical separation (i.e., each module is distinct) in the illustrated embodiment, wherein each module is implemented on an individual computer system. In one alternative to geographical separation, one or more modules comprise logically separable portions of a single computer system. In yet another alternative to physical separation of the modules, they are separated organizationally, wherein one organization operates one module and another organization operates a second. One of ordinary skill in the art will recognize that the greater the separation between client module 102 and modules within system 100, the greater the degree to which access to user information on client 102 or within system 100 may be constrained.

The greater the "need-to-know" of system 100 concerning user information on client 102, the weaker the nominal separation between client 102 and the modules of system 100. For example, in the monitor mode of operation discussed in the following section, system 100 has a relatively high need-to-know. Varying degrees of overlap are thus contemplated between the modules in alternative embodiments of the invention. In one alternative embodiment, one or more of the modules within system 100 are co-located. In yet a further alternative embodiment, client 102 overlaps or is co-located with one or more of the modules of system 100.

In a normal mode of operation in the embodiment of the invention depicted in FIG. 1, a user at client 102 registers (e.g., creates) an account with system 100 before conducting anonymous transactions. At the time of account registration, a pseudonym is chosen or

assigned to the user. Illustratively, the pseudonym also serves as the user's account name. Following the assignment of a pseudonym, two digital certificates are created. The first certificate (hereinafter termed "Cert1") is used to validate the user's identity to system 100 when he or she connects to the system to conduct an anonymous transaction. In this context, "identity" includes the user's confidential identity (which could, of course, include the user's true identity). Cert1 therefore advantageously eliminates the need for system 100 to retain the user's confidential identity while processing his transaction, thus maintaining his anonymity even within system 100. The second digital certificate (hereinafter termed "Cert2") is used to sign outgoing anonymous communications from the user (i.e., to imprint the communications with the user's pseudonym). In the presently described embodiment of the invention, client 102 generates or otherwise issues a first pair of asymmetric (i.e., public/private) keys, from which Cert1 is generated, and account module 110 generates or otherwise issues the second pair of keys, from which Cert2 is generated. The members of the first pair of asymmetric keys are hereafter termed PuK1 and PrK1, while the members of the second pair are termed PuK2 and PrK2.

When a registered user wishes to conduct an anonymous transaction or communicate anonymously with a third party, he or she again accesses system 100 through mask module 104 and establishes a user session. The user is then authenticated (using Cert1), and public keys corresponding to coordination module 106 and the operating modules are downloaded to client 102. Various pieces of information provided by the user and needed by system 100 to effect the transaction or communication are individually packaged and encrypted with the public keys of the operating modules that must act upon the information.

In one embodiment of the invention, the information necessary to conduct an anonymous transaction is separated into packages in accordance with instructions stored on client 102. For an outgoing electronic mail message, for example, client 102 packages the user's billing information (needed by billing module 108) separately from the body of the message (needed by action module 112 when acting as an outgoing mail server). The instructions illustratively allow client 102 to recognize the type of transaction and to create the appropriate packages.

A transaction identifier (e.g., a code identifying the type of transaction or communication) is then combined with the package(s) to form a "bundle," which is then encrypted with a public key of coordination module 106. Mask module 104 may remove any

information from bundles sent from the user to system 100 that may identify the user's true or confidential identity (e.g., IP address, electronic mail address) and forwards the bundles to coordination module 106.

Coordination module 106 decrypts each bundle to retrieve the transaction identifier and the individual packages of information. The packages are forwarded to the appropriate operating modules to conduct or process the indicated transaction. Each operating module illustratively receives only the information necessary to perform its discrete task (e.g., when sending electronic mail, billing module 108 receives the user's billing data, but not the content of the message or the recipient's confidential identity). Each operating module decrypts the package(s) sent from the coordination module and performs its specified task(s).

As stated above, in the presently described embodiment of the invention an outgoing communication is digitally signed by encrypting it with private key PrK2 corresponding to public key PuK2 in the second digital certificate Cert2. The pseudo-anonymous user's Cert2 is passed to the recipient along with the communication in this embodiment. The recipient may then authenticate the certificate by contacting account module 110 in its role as a CA. In an alternative embodiment of the invention, the digital signature is not computed on the communication per se, but on a message digest such as that created by "hashing." In this alternative embodiment, an outgoing communication is run through a hashing algorithm to produce a hash result (generally of fixed length). This result is then encrypted with the originating pseudo-anonymous user's PrK2 (illustratively stored on account module 110) to produce a message digest that is passed to the recipient along with the communication. The recipient decrypts the message digest using PuK2 (illustratively forwarded as part of Cert2) and processes the communication with the same hashing algorithm referred to above. If the result of the recipient's hashing algorithm matches the decrypted message digest, the recipient can be confident that the communication was not altered during its journey.

As described above, the presently illustrated embodiment of the invention employs public key encryption (PKE) methods (e.g., Diffie-Hellman, RSA, El Gamal) to safeguard information (e.g., details of anonymous communications and transactions) and to protect users' confidential identities. A user's confidential identity can only be retrieved in the "monitor" mode of operation described below. Once a pseudonym is chosen for a user and appropriate digital certificates are issued, the pseudonym is used to send and receive information to and from third parties.

In addition to the asymmetric keys associated with Cert1 and Cert2, in a present embodiment of the invention a symmetric (e.g., DES, RC4 by RSA) key may be used to encrypt a user's confidential (and/or true) identity, which is then stored on system 100. The symmetric key is illustratively retained on client 102 and is inaccessible to system 100 unless and until retrieved in accordance with the "monitor" mode of operation, in which case the key is retrieved and the user's identity decrypted and provided to an authorized entity. In an alternative embodiment of the invention, a symmetric key is used to encrypt and decrypt communications between client 102 and system 100 before Cert1 is issued.

One skilled in the art will thus appreciate that various methods and types of cryptographic security may be utilized within the scope of the invention.

Monitor Mode of Operation

In connection with the above-described embodiment of the invention, a "monitor" mode of operation may also be provided. While operating in this mode, system 100 may satisfy legal or other requirements of an entity authorized to retrieve the content of communications to and/or from a particular user (e.g., based upon the user's pseudonym or account name). When system 100 is placed in the monitor mode of operation for a particular user (e.g., in response to a court order), account module 110 stores an indicator (e.g., a flag or database entry) with or within the specified account, illustratively based on a pseudonym or account name provided by the entity.

As introduced above, in this embodiment the user's confidential identity (which could include the user's true identity), is stored on account module 110 in encrypted form (e.g., from the time of account creation). The confidential and/or true identities are encrypted with a symmetric key (e.g., as provided by DES) that is maintained only on client 102. When monitor mode is turned on in this embodiment, the key is retrieved from client 102 and the user's confidential and/or true identities are decrypted and provided to the entity (preferably, but not necessarily, being encrypted or otherwise secured prior to transmission to the entity).

In the event that a user's confidential identity must be recovered (e.g., because monitor mode is activated) but the user never re-connects to system 100, the encrypted identity or identities may still be provided to the monitoring entity. Although system 100 will not be able to decrypt or provide the decryption key for this information in the presently described

embodiment, the monitoring entity may possess the resources to overcome the cryptographic security and retrieve the desired information.

As was described in the previous section, the content of a user's communications are normally kept secure by encrypting portions of the content with public keys of one or more modules of system 100. In monitor mode, however, the content of the user's communications must be provided to the authorized entity. Advantageously, though, the entity is not given the modules' private keys in the presently described embodiment. Instead, system 100 (e.g., via coordination module 106) decrypts and records the user's communications and provides the content to the authorities. In order to make this possible, client 102 illustratively is sent, in place of the valid public keys of the operating modules that would be sent in a normal mode of operation, multiple copies of a public key of coordination module 106. Thus, when the user's information packages are encrypted by client 102, they are encrypted using the coordination module's key. When a bundle is received by coordination module 106 for dissemination to the operating modules, it is thus able to decrypt and record the contents of each package within the bundle. After recording the contents, they are re-encrypted with valid public keys of the operating modules (which were illustratively stored on coordination module 106) and the communication is thereafter handled normally.

Sometime after the details of the user's transaction are retrieved and recorded, they are passed to the authorized entity. In one embodiment of the invention, a separate public/private key pair may be generated to secure the details for transmission to the entity. Illustratively, coordination module 106 (or account module 110) generates the key pair. The private key is provided to the entity via some appropriately secure means (e.g., by hand, via Diffie-Hellman or other well-known key exchange protocols, by encryption with a second key) while the public key is retained by coordination module 106. The public key is then used to encrypt the details before they are sent to the entity, at which point the private key is used to retrieve them.

In one alternative embodiment of the invention, coordination module 106 avoids the possibility that a user or client 102 may observe the receipt of multiple identical keys, as described above, and thereby detect the activation of monitor mode. Specifically, for monitor mode operation in this alternative embodiment, coordination module 106 (or, for example, account module 110) generates a separate pair of public and private keys for each operating module for which client 102 is to receive a key. The public keys are then delivered to the client and the private keys are retained by coordination module 106 in order to access the contents of

the user's communications and transactions. Because the client receives different keys for each operating module, the activation of monitor mode is further concealed.

One of ordinary skill in the art will understand that cryptographic security of user's communications and transactions is thus ensured, on the one hand, by separately encrypting different portions of a user's communication or transaction. However, the cryptographic security can be breached, on the other hand, by providing a substitute for the operating modules' public keys, the complements (i.e., the corresponding private keys) of which are retained on system 100. The substitute may, of course, be substituted for less than all of the operating modules' keys, in which case certain information (e.g., billing data) will not be recovered.

In an alternative embodiment of the invention the user's confidential and/or true identities are encrypted with a public key of system 100, or one of its constituent modules, and stored on system 100 (preferably in a module other than the one whose key was used to encrypt the identities). When monitor mode is turned on, the encrypted identities are retrieved and decrypted using the corresponding private key. They may then be encrypted using a key specified by the monitoring entity before being delivered to the entity (e.g., account module 110 generates a separate pair of keys for securing communications between system 100 and the monitoring entity).

In another alternative embodiment, when the user next establishes a session with system 100 after monitor mode is activated, his or her confidential and/or true identities are retrieved from client 102. Illustratively, the identities are encrypted with a symmetric key or a public key of system 100 (or one of its modules) before being transmitted to system 100 from client 102.

Creating an Anonymous User Account

Before a user can send and receive anonymous communications through system 100, an account must be created to register the user and provide him or her a pseudonym. It is during this registration process that the two key pairs and digital certificates mentioned above are generated or otherwise obtained. An illustrative method of registering a user and establishing a pseudonym is described below with reference to FIG. 2. Briefly, however, the process may be summarized as follows.

A user at client 102 logs into system 100 through mask module 104 and chooses the type of account he wishes to establish. Depending upon the type of account chosen, the user's

true identity, or at least the confidential identity that is to be protected, is validated with a commensurate degree of confidence. If the user desires a highly trusted account with which to conduct electronic commerce, for example, his identity must be established with certainty in order to eliminate the danger of impersonation. After the user's identity (true and/or confidential) is verified, he chooses a pseudonym (e.g., a fictitious name) for his account. Mask module 104 communicates with account module 110 (through coordination module 106) to determine whether the desired pseudonym is already in use. Once a unique pseudonym is chosen (e.g., Anonymous123), client 102 generates via standard techniques known to those skilled in the art, or otherwise obtains (e.g., from a key issuer), a first pair of keys. The first private key ("PrK1") is retained on client 102 and the first public key ("PuK1") is delivered to account module 110. Puk1 is signed by system 100 to generate a first digital certificate ("Cert1"), which is then returned to client 102.

Account module 110 then generates or obtains a second pair of keys. The second private key ("PrK2") is stored on account module 110 and the second public key ("PuK2") and the user's pseudonym are signed with the system's private key to generate a second digital certificate ("Cert2"). Cert2 is also stored in account module 110.

The user is now registered and can send and receive anonymous communications and conduct pseudo-anonymous transactions through system 100. Cert1 is used to validate the user to system 100 whenever he wishes to establish a user session and use the system, and Cert2 is used to assert the user's anonymous identity (i.e., his pseudonym) to third parties and to receive communications sent to the user in his pseudo-anonymous identity.

With reference now to FIG. 2, an illustrative detailed description of this procedure is presented. State 200 is a start state. In state 202, a user at client 102 connects to, or logs into, mask module 104. In one embodiment of the invention client 102 is a web browser and state 202 involves the user accessing a web page corresponding to system 100. In an alternative embodiment, client 102 comprises a series of executable instructions provided by the operator of system 100, in which case the user simply operates the client software as instructed.

After connecting to mask module 104, in state 204 the user initiates the account creation process. Illustratively, this is accomplished by selecting a corresponding option from a list of functions or operations offered by system 100. In an alternative embodiment in which client 102 comprises software provided by the producer of system 100, the user's initial connection to mask module 104 automatically initiates the account creation process.

The user then, in state 206, chooses the type of account he desires. In a present embodiment of the invention, two types are possible: Type 1 and Type 2. Illustratively, a Type 1 account limits the associated user to basic anonymous transactions (e.g., those requiring a relatively low level of user authentication) such as electronic mail or web browsing. With a Type 2 account, the user may perform additional functions, such as electronic commerce. The type of account chosen by the user determines how thoroughly the user's identity (confidential and/or true) is validated. One skilled in the art will recognize that additional types of accounts may be provided in alternative embodiments of the invention or that the invention may even be limited to a single type of account.

In the presently described embodiment of the invention, if the user chooses a Type 1 account the account creation process jumps to state 210 below. In an alternative embodiment, the system will first verify (e.g., by querying the user), that the user is the only person with access to the electronic mail account that the user will use to send and received electronic mail using his pseudonym. In other words, because a Type 1 account is, in this embodiment of the invention, limited to sending and receiving electronic mail, it is sufficient to ensure that only the one user has access to the electronic mail account. This assurance is necessary in order to prevent the user from repudiating electronic mail sent from his account. In another alternative embodiment, the system simply contacts an identification server to verify an electronic mail account identified by the user (e.g., by invoking the verify command of a computer system's sendmail daemon).

Type 2 accounts allow additional types of anonymous transactions (e.g., electronic commerce). Therefore, it is not enough to ensure that the user is the only person accessing the user's account. If the user chooses a Type 2 account, system 100 ensures in state 208 that the user establishing the account is the person that he says he is. If the user's true identity were not validated, a dishonest person could create an anonymous account in the name of another person and make purchases in that other person's name, thus defrauding merchants and subjecting that person to unwarranted legal and financial disputes. In a present embodiment of the invention the user's true identity is authenticated by requiring a Class 2 digital certificate issued by VeriSign, Inc. or a comparable certificate from another trusted CA. The user transmits his authenticating certificate to system 100, where it can be validated in cooperation with the issuing CA. In an alternative embodiment, state 208 involves an alternate method of validating the user's true identity. Possible methods include, but are not limited to: requiring a user to

register an account in person, retrieving and examining a credit report, verifying a national identification card, using a biometric device (e.g., fingerprinting, retinal scan), or any other suitable method that may be developed.

Then, in state 210, the user selects a pseudonym. In the presently described embodiment, the pseudonym takes the form of an arbitrary or random name or other alphanumeric sequence and is also used as the user's account name. In an alternative embodiment, the pseudonym comprises some identifying information (e.g., electronic mail address) of the user other than his or her confidential identity. Illustratively, the user is prevented from choosing an offensive or otherwise inappropriate name. In addition, the user is prevented from choosing a pseudonym that may generate confusion concerning another person or entity. Alternatively, system 100 assigns the user a pseudonym instead of allowing the user to choose his or her own. In state 212 the chosen name is submitted to account module 110 for validation. In state 214 the account module consults a list (e.g., a database) of existing pseudonyms to determine if the user's choice is already in use. If the desired pseudonym is in use, the user is informed and the procedure returns to state 210. Otherwise, the procedure proceeds to state 216.

When a valid (e.g., unique) pseudonym is chosen or assigned, it is stored in memory on account module 110. Various types of memory are suitable for storing pseudonyms, including software constructs (e.g., list, table, array), storage media (e.g., disk, tape, compact disc) or solid-state memory. In the presently described embodiment of the invention, the pseudonym is used as an account name for the newly created account. In an alternative embodiment, however, a separate account name is assigned.

In state 216, client 102 generates a first pair of keys (one private key and one public key) in accordance with public key cryptography methods. In the presently described embodiment, client 102 includes the ability to generate key pairs. In an alternative embodiment, client 102 accesses a separate key generation utility or module to generate the keys. The first private key (PrK1) is retained by client 102 (illustratively, by being encrypted and stored on a storage device employed by the user). The first public key (PuK1) is, in state 218, transmitted by client 102 to mask module 104 and from mask module 104 is transmitted through coordinator 106 to account module 110. Additional data may be provided as well (e.g., user's date of birth, sex, geographical region of user's residence). In one embodiment of the invention, the additional information is incorporated in one or both of Cert1 and Cert2.

Account module 110, in state 220, digitally signs PuK1 and the user's pseudonym. Account module 110 thus creates a first digital certificate (Cert1) that will be provided by the user whenever he connects to system 100 to send or receive communications or to conduct transactions. Illustratively, the key with which Cert1 is signed is a private key representing system 100.

In state 222, Cert1 is returned to client 102 (through coordination module 106 and mask module 104) where it is stored with appropriate security. In an embodiment in which client 102 comprises software provided by the producer of system 100, Cert1 and PrK1 are stored in encrypted form and the user is required to provide a password or other means of authentication (e.g., fingerprint) to access and use either.

Account module 110 then, in state 224, creates a second pair of keys in accordance with public key cryptography. In state 226, the second private key (PrK2), which is used to digitally sign outgoing communications in one embodiment of the invention, is stored on account module 110. In state 228, the second public key (PuK2), along with the user's pseudonym and any additional data that may have been sent from client 102 (in state 218), is signed by system 100 to create a second digital certificate (Cert2). In one embodiment of the invention, Puk2 is provided (e.g., as part of Cert2) to a third party along with the anonymous user's communication so that the third party can validate the digital signature. Cert2 is then associated with the user's pseudonym and stored on account module 110 in step 230. The procedure then ends at state 232.

In the embodiment described above, Cert2 is issued at the time of account creation for use in all subsequent transactions with third parties on the user's behalf. In an alternative embodiment, Cert2 is dynamically generated when needed instead of being stored on account module 110. In this embodiment, PuK2 is consistently used to generate Cert2, but other information is included as needed. For example, in one transaction Cert2 could include the anonymous user's birth date. In another transaction, Cert2 could include other personal information, such as a geographic region in which the user resides.

In another alternative embodiment of the invention, only one pair of keys is generated during the account creation process (e.g., Cert1 and Cert2 are identical). This alternative embodiment provides a level of convenience but may sacrifice a portion of the user's anonymity (e.g., his IP address).

Once his account is created, the anonymous user simply connects to system 100, as needed, to establish a user session and conduct his or her anonymous transaction(s). One method of using system 100, as depicted in FIG. 1, to establish a user session and send an electronic mail message is depicted in the flow charts of FIGs. 3A-3B and 4A-4C.

Establishing a User Session to Conduct an Anonymous Transaction

FIGs. 3A-3B demonstrate an illustrative procedure by which an anonymous user having an account on system 100 establishes a user session in preparation for conducting an electronic transaction. In summary, before a transaction can be performed, the user must be authenticated. Illustratively, client 102 submits Cert1 (the first digital certificate created and described above) to the system. If Cert1 is deemed valid and the user's account has not been deactivated (e.g., for non-payment of a debt), the user receives one or more "operating module keys." Each operating module key is illustratively a public key associated with an operating module (e.g., billing module 108, action module 112). The user also receives a public key for coordination module 106.

The use of different operating module keys ensures greater security for user communications and transactions, in that no single module is able to determine the user's confidential identity or the full content of the user's message. However, in the monitor mode of operation a different public key (for which the corresponding private key is retained on system 100) is substituted for each operating module's actual key, thus breaching this security scheme so that communication contents can be provided to an authorized entity. As explained above, the substituted keys are illustratively generated by coordination module 106 and are different for each operating module. Alternatively, all of the substituted keys can be identical. In either case, the private key(s) corresponding to the substituted keys are held by coordination module 106 in order to decrypt communication bundles and retrieve their contents on behalf of a monitoring entity.

With reference now to FIGs. 3A-3B, an illustrative method of establishing an anonymous user session with system 100 is described. In the illustrated method, state 300 is a start state. In state 302 the user connects to, or logs into, mask module 104 using his pseudonym (and/or his account name if different from his pseudonym). In state 304 the client validates mask module 104; illustratively, mask module 104 passes client 102 a digital

certificate issued by a trusted certification authority. Client 102 may validate the certificate by contacting the CA.

Then, in state 306 a public key of coordination module 106 is provided to client 102. Client 102 uses this key to encrypt bundles of transaction details or communication content sent to coordination module 106. As described below, individual packages of information that, when assembled, constitute a bundle are encrypted with public keys (e.g., operating module encryption keys) corresponding to the operating modules that are to act upon the information. After the packages are encrypted, the entire bundle is encrypted with the public key of coordination module 106.

Each bundle that is encrypted with the coordination module's public key and submitted to coordination module 106 also includes a Transaction Type Code (TTC). The TTC represents the type of action the user is initiating (e.g., logging into the system, sending an electronic mail message, initiating an electronic purchase, retrieving electronic mail messages), and is retrieved by coordination module 106 by decrypting the bundle with its private key. As mentioned above, coordination module 106 can decrypt the bundle itself, but packages within the bundle (i.e., information destined for operating modules) cannot be decrypted because they are encrypted with the public keys of the operating modules. The corresponding private keys for the operating modules are held only by the individual modules.

With the coordination module's public key, in state 308 the client encrypts Cert1 and a login bundle (e.g., a bundle having a TTC corresponding to a login request). In state 310, the login bundle is delivered to mask module 104. Mask module 104 cannot retrieve any portion of the bundle but, in state 312, attaches a unique session identifier to the bundle. Mask module 104 does not forward any information indicating the anonymous user's confidential identity or other identifying information (e.g., IP address, electronic mail address).

The unique session identifier that mask module 104 creates for each user session allows system 100 to segregate communications involving different anonymous users. Although an anonymous user's account name or pseudonym may be able to serve the same purpose, one advantage of the presently illustrated method is to provide greater anonymity to the user within system 100. This reduces even further the possibility of linking the user's confidential identity with his pseudonym. For example, if billing module 108 were provided the user's pseudonym, that identity could be associated with the user's billing data (e.g., credit card number).

As described above, in the presently illustrated embodiment of the invention, the unique session identifier generated by mask module 104 is, within system 100, only used for communications passing between mask module 104 and coordination module 106. In one embodiment of the invention coordination module 106 generates additional identifiers for communicating with each operating module during a user session. This scheme further discourages the association of a particular communication or transaction with a particular identity (confidential or true). In an alternative embodiment only one unique session identifier is generated, such as that provided by mask module 104, and is used throughout system 100.

In state 314, the user's login bundle is delivered to coordination module 106. The coordination module then, in state 316, decrypts the bundle to retrieve the TTC and Cert1 and to note the session identifier. The coordination module next authenticates Cert1 and verifies the user's account in state 318 by querying account module 110. The account module will return an appropriate account status.

More specifically, in state 318, the account module informs coordination module 106 that Cert1 is either "Invalid" or "Valid," thus indicating the status of the user's account. In addition to an account status, account module 110 may also return a qualifier with the status. In a present embodiment of the invention, two qualifiers are employed for valid accounts: "monitor" and "collect." The "monitor" qualifier relates to the monitor mode of operation discussed above, and serves to inform the coordination module that the user's communications are to be monitored. The "collect" qualifier indicates that the user's account is due to be charged some amount (e.g., for continued use of system 100).

In one embodiment of the invention, upon receipt of the "collect" qualifier (and an associated sum that is due) coordination module 106 instructs billing module 108 to charge the user's credit card. Alternatively, coordination module 106 informs billing module 108 of the specified sum the next time a transaction is performed that involves the billing module, in which case the due sum is billed along with the transaction charge. In another alternative embodiment, coordination module 106 sends a message to client 102 to inform the user of the debt. Until the user returns payment information or makes other payment arrangements, system 100 performs no more anonymous transactions on the user's behalf (except perhaps to accept electronic communications from third parties – which are not delivered until payment is received).

In state 320, coordination module 106 receives the status information from account module 110. If the account is valid, the illustrated method continues at state 326. If, however, the account is considered invalid (e.g., the account has been closed or deleted), the coordination module composes a message to client 102 in state 322 to inform it (and the user) of this status. This message is illustratively encrypted with PuK1 (from Cert1). The "invalid" bundle is delivered to the client in state 324, after which the procedure ends in end state 340.

In state 326, coordination module 106 elicits and receives a public key from each operating module (e.g., billing module 108, account module 110 and action modules 112, 114 and 116). Advantageously, each operating module generates a new pair of keys (i.e., one private and one public) for each unique session identifier. Additionally, in one embodiment of the invention the public keys used by coordination module 106 and the operating modules are changed on a regular basis during a session (illustratively, new keys are generated every hour). Illustratively, however, old keys are valid for a limited period of time after new ones are generated (e.g., five minutes). Alternative mechanisms of handling the transition between keys are possible. For example, use of the old keys may be rejected immediately upon generation of the new ones, in which case client 102 may be forced to re-send information directed to the operating modules during the transition.

Then, in state 328, coordination module 106 determines whether monitor mode is active for the user. As described above, this information becomes available to coordination module 106 during the attempted validation of the user's account. If monitor mode is not active, the process continues at state 334. If, however, monitor mode is active, in state 330 the coordination module stores the public keys received from the operating modules. Then, in state 332 coordination module 106 generates a new pair of public and private keys for each operating module that provided a public key in state 326. The private keys are retained on coordination module 106. In an alternative embodiment of the invention, in state 332 coordination module 106 assembles copies of its public key to substitute for the operating modules' keys that were provided in state 326.

In state 334 the coordination module assembles either the operating modules' public keys (if monitor mode is not active) or the substitute public keys (if monitor mode is active) into a "success" bundle. This bundle will be returned to the client 102 to inform the user that a user session has been established. In an exemplary embodiment of the invention, the keys

provided to client 102 are termed "operating module encryption keys" regardless of whether they constitute the operating modules' actual public keys or substitutes therefor.

In state 336, the "success" bundle is encrypted with the user's PuK1. This bundle can thus only be decrypted with PrK1, the private key corresponding to PuK1, which is stored on client 102. In state 338, the success bundle is delivered to client 102 where it will be decrypted and understood to indicate that the user has been validated and that a user session (and a unique session identifier) has been established. The process then exits in end state 340.

It will be recalled that when monitor mode is active for an anonymous user's account, the contents of the user's transactions and communications are provided to an authorized entity. To make this possible, substitute keys were generated and provided to client 102 in place of the operating modules' actual keys. Therefore, instead of encrypting information packages for the operating modules with their actual public keys, client 102 encrypts each package with the substitute keys. Coordination module 106 possesses the complementary keys for the substitutes and is thus able to easily retrieve the contents of the user's communications, which are then recorded or transmitted to the authorized entity. Illustratively, the public keys of the operating modules are stored by coordination module 106 so that the coordination module can encrypt the information packages before forwarding them to the operating modules. One of ordinary skill in the art will recognize that information packages sent to the operating modules after being opened by coordination module 106 are preferably encrypted with their own public keys in order to avoid requiring them to store additional keys. In addition, the scheme described above leaves the operating modules unaware that a user's transactions are being monitored.

In an alternative embodiment, the encrypted bundles of a monitored user, or just the encrypted information packages, are passed to the monitoring entity along with the key(s) necessary to decrypt the information. In another alternative embodiment of the invention, the operating modules' actual public keys are provided to client 102 in state 334 regardless of whether monitor mode is active. In this embodiment, coordination module 106 must then retrieve the operating modules' private keys in order to decrypt the information packages (the contents of which are then recorded, re-encrypted and forwarded). Or, the recording of transaction/communication details is done by the individual operating modules. This alternative is relatively dissatisfactory because it requires additional time and action on the part of coordination module 106 and/or the operating modules.

Processing an Anonymous Transaction

FIGs. 4A-4C demonstrate an illustrative procedure for using system 100 to send an electronic communication from an anonymous user after a user session is established. As stated above, the user receives separate public keys with which to encrypt information packages for each operating module, thus providing each module with only the information necessary to conduct its role in the overall transaction. The packages are, in the illustrated procedure, assembled into a bundle that is encrypted with a public key of coordination module 106. In a monitor mode of operation according to one embodiment of the invention, however, the public keys of the operating modules are replaced by substitute public keys generated by the coordination module. In an alternative embodiment, the substitute keys are identical and illustratively match the coordination module's public key.

The information needed to send a message is, as described above, separated into packages (e.g., electronic mail message, billing information) destined for individual operating modules. The bundle of packages is transmitted to the coordination module where it is divided and the separate packages forwarded to the appropriate modules. In other words, the billing information package is submitted to the billing module, the communication or transaction content is submitted to an action module, etc. In the monitor mode of operation the coordination module decrypts and records each package of information before re-encrypting them (with the operating modules' valid public keys) and forwarding them to the operating modules. Each operating module then, under the coordination of coordination module 106, performs its task(s) using the provided information.

In the embodiment depicted in FIGs. 4A-4C, action module 112 is an operating module configured to send electronic mail. The illustrated procedure begins with start state 400. In state 402 the user initiates a transaction. For example, to send an electronic mail message, after the user composes the message he signals completion by clicking on a "send" button or similar icon.

Client 102 then, in state 404, encrypts the information needed to bill the user for the message (e.g., credit card or digital cash account number). As discussed with reference to FIGs. 3A-3B, client 102 received public keys ostensibly supplied by each of the operating modules. This information package is therefore encrypted using the key associated with billing module 108. However, as described previously, in a monitoring mode of operation this key may have been replaced with a public key of, or generated by, coordination module 106.

In state 406, client 102 encrypts the information (e.g., body of mail message, recipient identity) to be sent to action module 112 with the public key corresponding to the action module.

In state 408, client 102 assembles the various information packages into a bundle and adds a Transaction Type Code (TTC) corresponding to the function of sending electronic mail. Then the client encrypts the bundle in state 410 with the public key of coordination module 106 and delivers the bundle to mask module 104 in state 412.

Next, in state 414 the mask module attaches to the bundle the session identifier that was generated when the user's session was established, and forwards the bundle to coordination module 106. The coordination module decrypts the bundle with its private key in state 416 and retrieves the TTC.

Based on the TTC, in state 418 the coordination module calls a transaction handler routine and passes it the decrypted bundle (comprised of one or more encrypted information packages destined for one or more operating modules). Illustratively, coordination module 106 includes a separate transaction handler routine to coordinate each type of transaction. Each transaction handler is thus configured to forward information packages to the appropriate operating modules without decrypting them or otherwise knowing their contents (except in the monitor mode of operation). It will be recalled that different session identifiers are illustratively generated for each communication sent between coordination module 106 and the operating module.

Additional action must be taken if monitor mode is active for the user. In particular, the contents of the user's transaction must be recorded for (or directly transmitted to) an authorized monitoring entity.

In state 420, coordination module 106 determines whether monitor mode is active. Illustratively, the coordination module was provided with this information at the time that the user session was established. When, however, monitor mode is activated during a user session, the next time the operating modules' public keys are changed the coordination module will substitute its public key (or those it generates) for the operating modules' keys. As described above, coordination module 106 stores the operating modules' public keys in monitor mode in order to re-encrypt the information packages after recording them. In one alternative embodiment of the invention, when monitor mode is activated during a user session the operating modules are automatically prompted to issue new public keys. In another alternative

embodiment, when monitor mode is activated during a user session, it does not take effect until the user's next session.

If monitor mode is not active, the process continues with state 426. However, if monitor mode is active, in state 422 coordination module 106 (e.g., the transaction handler routine) decrypts and logs (e.g., records) the contents of each information package. Then, in state 424, the coordination module (e.g., transaction handler routine) re-encrypts each information package using the stored public key of the operating module to which the package is to be delivered.

In state 426 the billing package is delivered to billing module 108, which decrypts and processes the billing data in state 428. While processing the billing data, the billing module may be required to make or use a connection to third parties such as credit card issuers, banks, value acquirers, etc. Illustratively, billing module 108 receives only the information necessary to charge the user for the transaction, which may include a portion of the user's confidential identity (e.g., where the confidential identity includes the user's true name, which is necessary for credit card billing) but does not learn the user's pseudonym. Alternatively, billing module 108 could receive all or substantially all of the contents of the encrypted bundle sent from client 102. Non-billing information remains safe, however, as the billing module normally does not possess the key(s) necessary to decrypt any information other than its billing information.

In state 430, the transaction handler routine determines whether the billing data was successfully processed. If not, an error is returned to client 102 in state 432 at which point the process ends at end state 460.

If the billing data is successfully processed, then in state 434 the coordination module (e.g., the transaction handler routine) passes the action package to action module 112. The action module decrypts the package in state 436 and processes the action information (e.g., recipient of the message, message text, sender's pseudonym). If action module 112 determines in state 438 that the outgoing electronic mail message is complete, the process continues at state 448. When, however, additional information is needed (e.g., no recipients are identified or the message indicates that an attachment should be included but no attachment was sent in the package), the action module informs coordination module 106. The coordination module then, in state 440, sends a message to client 102 requesting the additional information. In state 442, the additional information is encrypted with the public key associated with action module

112 (which may, of course, be the coordination module's public key) and the information is delivered in state 444. Illustratively, this additional information is transmitted in the same manner as other information (e.g., within a package inside a bundle that is encrypted with the coordination module's public key and sent to the coordination module). Action module 112 decrypts the additional information in state 446 and assembles the outgoing message.

Action module 112 now has the complete contents of the outgoing message. The message must, however, be digitally signed, illustratively by using Cert2 (e.g., PuK2). Thus, the body of the outgoing message is passed to account module 110 in state 448. In one embodiment of the invention, the body of the message is encrypted by action module 112 with a public key of account module 110. The encrypted body is then passed back to coordination module 106 with a code (e.g., a TTC) specifying the need for a digital signature. Coordination module 106 then passes the message body to account module 110.

Upon receipt, account module 110 digitally signs the message in state 450 and returns the signed message to action module 112 in state 452 (e.g., by encrypting it with a public key of the action module and passing it back through the coordination module). In one embodiment of the invention, the message is signed by appending a message digest to the message (e.g., generating a hash value from the message and encrypting it with PrK2).

In state 454, the action module determines whether a public key or digital certificate is available for the recipient. If not, the process continues at state 458. Otherwise, the outgoing message is encrypted in state 456 using the recipient's stored public key. The outgoing message is transmitted to the recipient in state 458. The process ends with end state 460.

In one alternative embodiment of the invention, action module 112 maintains a record of recipients to whom electronic mail is not to be sent (e.g., recipients who have requested not to receive electronic mail sent from one or more anonymous users). Illustratively, a global list is maintained to identify electronic mail addressees who are not to receive electronic mail from any anonymous user of system 100. Individual lists are also maintained in this embodiment for each valid user account, as necessary, to identify the addressees that are not to receive mail from the individual user. The individual lists may duplicate the global list or, alternatively, simply include addressees not included in the global list. In this alternative embodiment, action module 112 consults either or both of these lists prior to sending the message to account module 110 for signature. Recipients included in either list are stricken from the message and,

if any valid recipients remain, the procedure continues normally. The user is notified of any recipients that were removed from his specified addressees.

The procedure described above involves a single recipient. When an outgoing electronic mail message is addressed to multiple recipients it may be processed in a different manner. In one embodiment of the invention, for example, multiple copies of the outgoing message are created, each one addressed to an individual recipient. Each message is then processed as described above.

In an alternative embodiment with multiple recipients, however, separate copies of the message are created only for recipients having an encryption key (e.g., a public key of an asymmetric key pair) stored on system 100. Thus, one copy of the signed message is sent to all recipients for whom no key is available. For each other recipient, a copy of the signed message is encrypted with the recipient's key before being transmitted.

Receiving a Communication for an Anonymous User

In addition to initiating transactions and communications, system 100 also receives messages and communications for anonymous users from third parties. In an exemplary embodiment of the invention, billing activity is directed to billing module 108, while validation of messages sent by system 100 on behalf of anonymous users is performed by account module 110. When, however, messages (e.g., electronic mail) or transaction details are sent to a user, they are received by an action module.

FIG. 5 depicts an illustrative method of receiving an electronic mail message for a user of system 100 from a third party. In the illustrated embodiment, users and third parties need not alter their methods of initiating, receiving and responding to electronic mail messages. For example, a third party responds to an electronic mail message from a user by clicking on a "respond" button or issuing a comparable command. Similarly, in composing or addressing a new mail message to an anonymous user, a third party need not alter his or her normal practices. The third party simply addresses the message to the appropriate pseudonym (e.g., Anonymous123@Privada.Net).

In the illustrated embodiment, action module 114 is configured to receive inbound electronic mail. In an alternative embodiment, action module 112, which handled outgoing electronic mail messages, also receives incoming messages.

With reference now to FIG. 5, state 500 is a start state. In state 502, action module 114 receives an electronic mail message addressed to a pseudonym from a third party. Illustratively, action module 114 is coupled to the Internet or other wide-area network via a communication line.

Action module 114 then queries account module 110, in state 504, to determine whether the indicated pseudonym corresponds to a valid account on system 100. If not, action module 114 is so informed and, in state 506, returns the message to the sender. After state 506, the process completes with end state 522.

In a present embodiment of the invention, if an account exists for the addressed pseudonym but is currently considered "invalid," the message is accepted and stored but will not be retrievable by the associated user until her account status is changed to "valid." Alternatively, the message is simply rejected if the addressed account is "invalid."

After determining that system 100 maintains an account for the addressee in state 504, in state 508 it is determined whether the user accepts messages from the originating third party. In the presently described embodiment, a list is maintained (illustratively on account module 110) of third parties from whom a user does not wish to receive messages. If the originating third party is included in this list, the message is returned to the sender in state 506, possibly with a message indicating that the user does not exist or does not wish to receive messages from the sender. In alternative embodiments of the invention, multiple lists of unwanted message senders are maintained, such as one for each user or some combination of global or semi-global lists along with individual lists.

Although states 504 and 508 are depicted separately in the illustrated embodiment, in one embodiment of the invention account module 110 examines the validity of the user's account in conjunction with determining whether the user accepts messages from the third party.

In state 510 it is determined whether monitor mode is active for the addressee. In one embodiment of the invention, this determination is made concurrently with either of both of states 504 and 508. For example, in response to the query in state 502, account module 110 returns a message indicating that the addressee account is valid but monitored.

If the addressee's account is not being monitored, the process continues at state 514. If, however, the account is being monitored, the process continues in state 512. In state 512, a copy of the message is made (e.g., by action module 114) and encrypted with a public key of

the monitoring entity. As described above, when monitor mode is activated for an account, in one embodiment of the invention a pair of asymmetric keys (e.g., one public, one private) is generated (illustratively by account module 110). The private key is provided to the entity authorized to monitor the subject account, and the public key is used to encrypt communications and transaction details as they are processed by coordination module 106. When receiving an electronic mail message, however, in the presently illustrated embodiment of the invention action module 114 (e.g., rather than coordination module 106) applies the entity's public key to encrypt the message copy.

In state 514 action module 114 encrypts the received message with PuK1 (from Cert1). Next, in state 516 action module 114 stores the message in a file having a file name unique from all other stored messages (illustratively, the file name includes a time stamp). All messages received by action module 114 for users of system 100 are, in one embodiment, stored in a common area. This practice helps prevents anyone who may gain access to this pool of messages from determining which, or how many, messages are received for a particular anonymous user.

The unique file name corresponding to the message is forwarded in state 518 to account module 110. The file name is then stored in state 520 with some association to the recipient's pseudonym. In one embodiment of the invention an array, indexed by account name, is maintained. As messages are received for a particular pseudonym, the file names of the messages are stored in the array. In an alternative embodiment of the invention, the file names are stored in a location other than account module 114 (e.g., coordination module 106). The process ends with end state 522

FIG. 6 depicts an illustrative procedure in which a user retrieves her electronic messages from system 100. State 600 is a start state. In state 602, the user logs into system 100 and establishes a user session. One method of establishing a user session is discussed above with reference to FIGs. 3A-3B. Then, in state 604, client 102 forwards a bundle to coordination module 106 having a TTC indicating that the user wishes to receive her electronic mail.

In state 606, a transaction handler passes the request (e.g., a package containing the user's pseudonym) to account module 114, which responds by sending a list of stored messages to client 102. In the presently illustrated embodiment of the invention, a short description (e.g., subject line, originator) of each message is saved on account module 114 with the unique file

names. Thus, account module sends some information concerning each mail message to client 102. In an alternative embodiment, account module 110 and action module 114 work in tandem to provide short descriptions to client 102. Illustratively, in this alternative embodiment action module 114 generates the identifying information in response to a request from account module 110.

In state 608, the user selects one or more messages to download. In state 610, client 102 sends a request to account module 110 (via coordination module 106) for some or all of the messages stored for the user. Account module 110 then, in state 612, retrieves the selected messages from action module 114 and sends them to client 102.

Upon receipt, client 102 decrypts the messages in state 614 using PrK1. The procedure then ends in end state 616.

In the procedure described above, the incoming electronic mail message was addressed to only a single user or pseudonym. The procedure may be altered in the event the message is addressed to multiple users. For example, in one embodiment, a separate message file is created to store a copy of the message for each user listed as an addressee. Each such file has a unique name or identifier, as in the procedure above. After the message is copied and stored in multiple files, the remainder of the message retrieval procedure is the same as described above.

The foregoing descriptions of embodiments of the invention have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the invention to the forms disclosed. Accordingly, many modifications and variations will be apparent to practitioners skilled in the art.

In particular, two possible action modules have been described, for sending and receiving electronic mail, respectively. In alternative embodiments of the invention, other modules are provided. For example, an action module for outbound news is within the scope of the invention. An outbound news module illustratively receives a message package from a user at client 102 (through mask module 104 and coordination module 106). The message is passed to the account module where it is digitally signed (e.g., with the user's PrK2) and returned to the outbound news module. The outbound news module then posts the signed message to the newsgroup or other location specified by the user.

An action module in another embodiment of the invention serves as a web proxy. A web proxy module illustratively provides a user access to Internet web servers (e.g., to view

web pages). The web proxy module does not know the confidential or true identities of the user, or his IP address, but does know the user's pseudonym or account name. In addition, should a web server require validation of a pseudonym, the web proxy module supplies the web server with the user's Cert2, which can be validated by account module 110.

In yet another embodiment of the invention, a commerce module is provided to enable anonymous electronic transactions through system 100. A commerce module illustratively learns the identity of the merchant that the user is dealing with, the price(s) of goods/services, a description of what is being purchased or sold, etc. In a present embodiment, the commerce module retains only limited knowledge of the anonymous user (e.g., just the user's pseudonym) and uses billing module 108 to make payments to merchants. A unique transaction identifier is illustratively generated by the commerce module for use in tracking an order, arranging delivery of a purchase, or retrieving details of the transaction.

In view of these and other alternative embodiments of the invention, the scope of the present invention is intended to be limited only by the terms of the claims below.

What Is Claimed Is:

1. A method of relaying an electronic communication between a user and a third party, where said user remains pseudo-anonymous to said third party, but where said third party is cryptographically assured of a pseudo-anonymous identity of said user, comprising:

(a) at an electronic intermediary, receiving:

(i) an electronic communication from a user to a third party with whom said user wishes to communicate without revealing a confidential identity of said user to said third party; and

(ii) a first digital certification of said user for said intermediary;

(b) authenticating said user to said intermediary by cryptographically verifying said first digital certification;

(c) assuring said communication for said third party by cryptographically signing said communication under a pseudonym of said user with an asymmetric cryptographic key associated with said pseudonym; and

(d) transmitting said cryptographically signed communication to said third party;

said signed communication being cryptographically authenticatable by said third party yet unusable by said third party to determine said confidential identity of said user.

2. The method of claim 1, further comprising account creation prior to said steps (a) and (b), said account creation comprising:

(x) verifying a confidential identity of said user;

(y) creating a second digital certification associated with said pseudonym, said second certification including a digital signature by said intermediary and usable by said third party to cryptographically verify said pseudo-anonymous identity of said user; and

(z) associating said pseudonym of said user with said second certification in a memory.

3. The method of claim 2 where said step (d) includes appending said second digital certification associated with said pseudonym to said signed communication.

4. The method of claim 1 further comprising creating said first digital certification by digitally signing a first asymmetric cryptographic key associated with said pseudonym.

5. The method of claim 4 where said first digital certification is verifiable only by said intermediary.

6. The method of claim 1 where:
said step (a) is performed by a masking module within said intermediary;
said step (b) is performed by a coordination module within said intermediary; and
said steps (c) and (d) are performed by one or more operating modules.

7. The method of claim 6 where said masking module is nominally separated from said coordination and operating modules, to constrain access to user information in said step (a) by said coordination and operating modules.

8. The method of claim 7 where said constrained access is controllable on a need-to-know basis.

9. The method of claim 6 further comprising generating a first unique session identifier to identify said communication to said coordination module.

10. The method of claim 9, wherein said first unique session identifier is generated by said masking module, further comprising:
generating a second unique session identifier at said coordination module to identify said communication to one of said one or more operating modules.

11. The method of claim 6 further comprising, between said steps (b) and (d):
(b') delivering a cryptographic key of one of said modules to a client module; and
(b") receiving, from said client module, a portion of said communication digitally signed with said delivered key.

12. The method of claim 11 where:
said delivered key is of said operating module; and
said steps (b') and (b") ensure privacy of said portion of said communication against said coordination module.

13. The method of claim 11 where said delivered key is of said coordination module, thereby breaching privacy of said communication to said coordination module; and further comprising digitally signing said communication at said coordination module with a cryptographic key of said operating module.

14. The method of claim 11 where said delivered key is generated by said coordination module, thereby breaching privacy of said communication to said coordination module; and further comprising digitally signing said communication at said coordination module with a cryptographic key of said operating module.

15. The method of claim 13 further comprising transmitting said communication to an external party on a need-to-know basis.

16. The method of claim 11 further comprising electing to ensure or breach privacy of said communication to said coordination module by selectively delivering said cryptographic key of one of said modules.

17. The method of claim 13 further comprising, prior to said step (a), creating in one of said client module and an account module a selectively disclosable record of a true identifier of said user by archiving, in encrypted form, information pertaining thereto.

18. The method of claim 17 where said archiving includes, before said step (a):
receiving an encrypted identifier of said user from a client module that stores, in a manner that is nominally inaccessible to other said modules, a decryption key usable to decrypt said encrypted true identifier.

19. The method of claim 18 further comprising, at said coordination module, obtaining said decryption key from said client module and decrypting said encrypted true identifier using said decryption key.

20. The method of claim 2 where said first digital certification and said second digital certification are the same.

21. The method of claim 1 further comprising verifying said communication against a plurality of authorized actions before said transmitting to said third party.

22. The method of claim 1 where said communication includes an electronic mail message.

23. The method of claim 1 where said communication includes a purchase request.

24. The method of claim 23 further comprising initiating a billing activity in response to said purchase request.

25. The method of claim 1 where said user accesses said electronic intermediary over a public network.

26. The method of claim 1 further comprising:

(e) receiving a response from said third party to said pseudonym of said user;

(f) storing said response for subsequent access by said user; and

(g) allowing said user to access said response.

27. The method of claim 26 further comprising, between said steps (f) and (g):

(f') receiving said first digital certification from said user; and

(f") authenticating said user by cryptographically verifying said first digital certification.

28. The method of claim 11 where said client module is implemented on a computer system of said user.

29. The method of claim 1 where said user accesses said electronic intermediary as a client-server process.

30. The method of claim 2 where said first and said second digital certifications are X.509 digital certificates.

31. The method of claim 1 where said step (a) is performed by a masking module within said intermediary, and said steps (b), (c) and (d) are performed among one or more operating modules that are cryptographically isolated from said masking module, thereby preventing transfer of certain confidential user information from said client module to said operating modules.

32. The method of claim 31 including at least two operating modules that are cryptographically isolated from each other, thereby preventing sharing of certain information therebetween.

33. A computer readable storage medium storing instructions that, when executed by a computer, cause a computer to perform a method for relaying an electronic communication between a user and a third party, wherein said user remains pseudo-anonymous to said third party, but wherein said third party is cryptographically assured of a pseudo-anonymous identity of said user, the method comprising:

(a) at an electronic intermediary, receiving:

(i) an electronic communication from a user to a third party with whom said user wishes to communicate without revealing a confidential identity of said user to said third party; and

(ii) a first digital certification of said user for said intermediary;

(b) authenticating said user to said intermediary by cryptographically verifying said first digital certification;

(c) assuring said communication for said third party by cryptographically signing said communication under a pseudonym of said user with an asymmetric cryptographic key associated with said pseudonym; and

(d) transmitting said cryptographically signed communication to said third party; said signed communication being cryptographically authenticatable by said third party yet unusable by said third party to determine said confidential identity of said user.

34. An electronic intermediary for relaying a communication between a user having a pseudo-anonymous identity and a third party, wherein said pseudo-anonymous identity is cryptographically authenticatable, comprising:

an interface for receiving said communication, and a first digital certificate, from said user;

an accounting mechanism for digitally signing said communication with a second digital certificate pertaining to said pseudo-anonymous identity; and

a first operating mechanism for transmitting said signed communication to said third party;

whereby said third party, upon receipt of said signed communication, may validate said communication by cryptographically authenticating said second digital certificate.

35. The electronic intermediary of claim 34, further comprising a coordination mechanism for coordinating processing of said communication in a first mode of operation and for monitoring said communication in a second mode of operation.

36. The electronic intermediary of claim 35, wherein one of said accounting mechanism, first operating mechanism, and coordination mechanism comprises said interface.

37. The electronic intermediary of claim 34, further comprising a billing mechanism to bill said user for relaying said communication.

38. The electronic intermediary of claim 34, wherein said communication pertains to a transaction, further comprising a second operating mechanism for interfacing with said third party to conduct said transaction therewith, wherein said user is identified to said third party only by said pseudo-anonymous identity.

39. A method of processing an electronic communication from a user having a pseudo-anonymous identity, said pseudo-anonymous identity being used in place of a confidential identity, comprising:

receiving a first digital certificate of said user via a client module;

authenticating said first digital certificate;

receiving a communication bundle from said user via said client module, said communication bundle including said electronic communication;

decrypting said communication bundle to retrieve said electronic communication;

submitting said electronic communication to an operating module, said operating module comprising a sequence of operating instructions to transmit said electronic communication to a third party;

digitally signing said electronic communication with a cryptographic key associated with a second digital certificate; and

transmitting said electronic communication and said second digital certificate to said third party in accordance with said operating instructions;

wherein said second digital certificate is cryptographically authenticatable by said third party to validate the electronic communication.

40. The method of claim 39, further comprising, prior to receiving said first digital certificate, creating an account for said user.

41. The method of claim 40, wherein said creating comprises:

verifying said confidential identity;

receiving said first digital certificate, said first digital certificate including said confidential identity; and

generating said second digital certificate, said second digital certificate including said pseudo-anonymous identity.

42. The method of claim 41, in which said second digital certificate further includes an identifying characteristic of said user other than said confidential identity.

43. The method of claim 39, further comprising, after receiving said communication bundle:

generating said second digital certificate to include an identifying characteristic of said user associated with said electronic communication.

44. The method of claim 43, wherein a replacement second digital certificate is generated for a subsequent electronic communication from said user.

45. The method of claim 39, wherein said authenticating comprises receiving a status of an account associated with said user.

46. The method of claim 45, wherein said authenticating further comprises receiving a qualifier of said account status.

47. The method of claim 39, wherein said receiving a communication bundle comprises associating a first session identifier with said communication bundle.

48. The method of claim 47, wherein said first session identifier is generated by a masking module, further comprising:

receiving said communication bundle and said first session identifier at a coordination module;

associating a second session identifier with a portion of said communication bundle; and

submitting said portion of said communication bundle and said second session identifier to said operating module;

wherein one of said first session identifier and said second session identifier is used to discern said communication bundle from a communication bundle of another user.

49. The method of claim 39, further comprising:

providing a bundle encryption key to said client module for encrypting said communication bundle; and

providing a first operating module encryption key to said client module for encrypting said electronic communication.

50. The method of claim 49, wherein said decrypting said communication bundle comprises:

decrypting said communication bundle with a bundle decryption key; and

identifying said electronic communication;

wherein said electronic communication cannot be decrypted with said bundle decryption key.

51. The method of claim 50, wherein said digitally signing comprises:

decrypting said electronic communication with an operating module decryption key; and

adding a message digest to said electronic communication.

52. The method of claim 49, wherein said bundle encryption key and said first operating module encryption key are identical.

53. The method of claim 49, wherein one of said bundle encryption key and said first operating module encryption key are generated by a coordination module.

54. The method of claim 49, wherein said decrypting said communication bundle comprises:

decrypting said communication bundle; and

decrypting said electronic communication.

55. The method of claim 54, further comprising encrypting said electronic communication with an encryption key different from said first operating module encryption key.

56. The method of claim 54, wherein said decrypting the electronic communication comprises:

receiving an operating module decryption key from said operating module; and

decrypting said electronic communication with said operating module decryption key.

57. The method of claim 54, further comprising providing the electronic communication to an external party on a need-to-know basis.

58. The method of claim 39, wherein said transmitting comprises encrypting said electronic communication with a cryptographic key of said third party.

59. The method of claim 39, further comprising:

receiving a message to said pseudo-anonymous identity at a receiving operating module;

encrypting said message with a cryptographic key associated with said first digital certificate;

storing said encrypted message; and

forwarding said encrypted message to said client module.

60. The method of claim 59, wherein said storing comprises storing said encrypted message in a manner such that said encrypted message cannot be readily associated with either of said pseudo-anonymous identity and said confidential identity.

61. The method of claim 39, further comprising storing a selectively retrievable identity of said user.

62. The method of claim 61, wherein said selectively retrievable identity is encrypted, further comprising receiving a decryption key usable to decrypt said identity.

63. The method of claim 62, wherein said decryption key is received from said client module.

64. The method of claim 62, further comprising:

retrieving said identity;

decrypting said identity; and

providing said identity to an external party on a need-to-know basis.

65. A computer instruction signal embodied in a carrier wave carrying instructions that, when executed by a computer, perform a method for relaying an electronic communication between a user and a third party, where said user remains pseudo-anonymous to said third party, but where said third party is cryptographically assured of a pseudo-anonymous identity of said user, the method comprising:

receiving an electronic communication to a third party from a user wishing to be known by a pseudo-anonymous identity in place of a confidential identity;

receiving a first digital certificate from said user;

authenticating said user by cryptographically verifying said first digital certificate;

cryptographically signing said communication using an asymmetric cryptographic key associated with said pseudo-anonymous identity of said user; and

transmitting said cryptographically signed communication to said third party;

wherein said cryptographically signed communication is cryptographically authenticatable by said third party without revealing said confidential identity of said user.

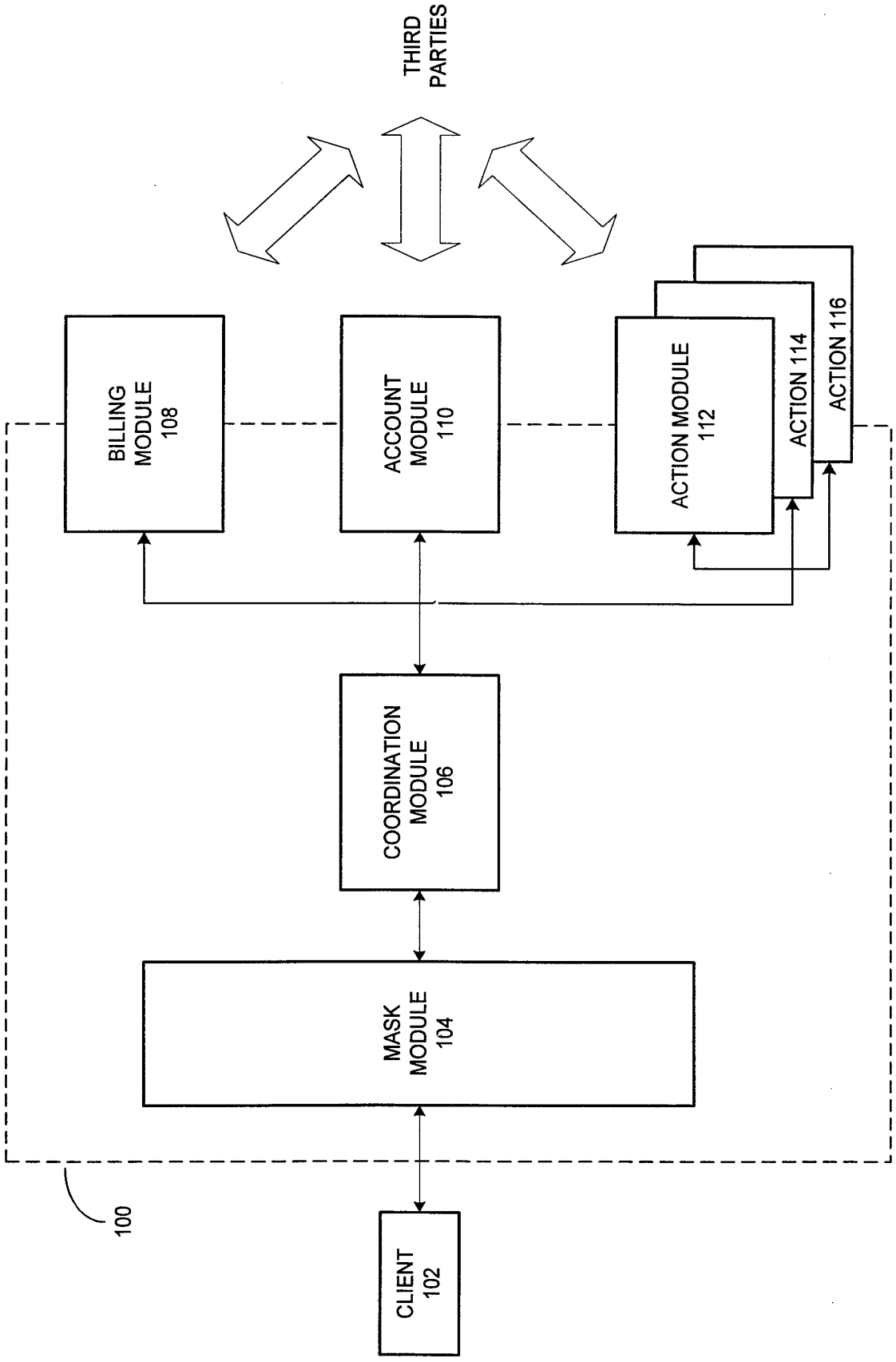

THIRD PARTIES
BILLING MODULE 108
ACCOUNT MODULE 110
ACTION MODULE 112
ACTION 114
ACTION 116
COORDINATION MODULE 106
MASK MODULE 104
CLIENT 102
100

FIG. 1

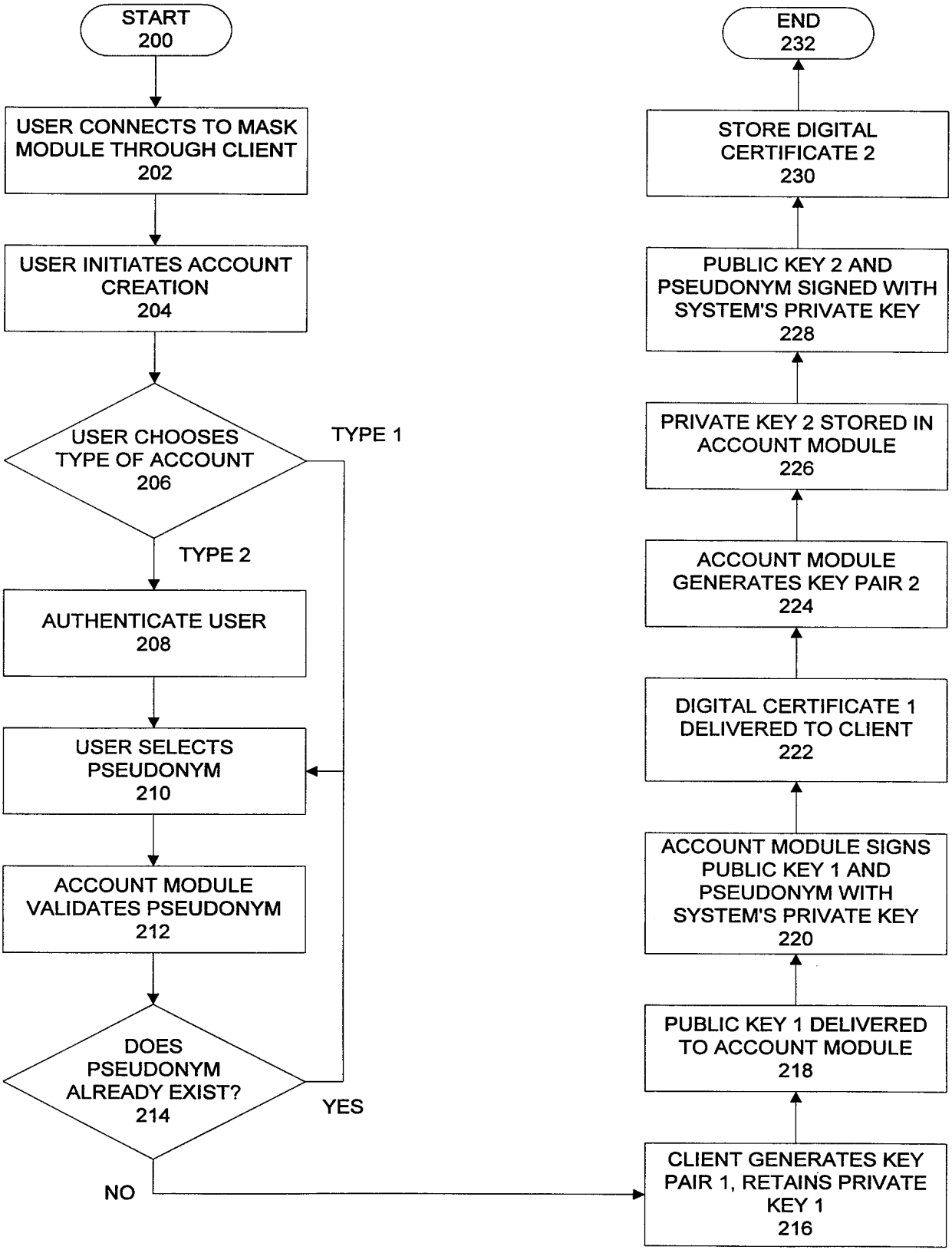

START
200
USER CONNECTS TO MASK MODULE THROUGH CLIENT
202
USER INITIATES ACCOUNT CREATION
204
USER CHOOSES TYPE OF ACCOUNT
206
TYPE 1
TYPE 2
AUTHENTICATE USER
208
USER SELECTS PSEUDONYM
210
ACCOUNT MODULE VALIDATES PSEUDONYM
212
DOES PSEUDONYM ALREADY EXIST?
214
YES
NO
CLIENT GENERATES KEY PAIR 1, RETAINS PRIVATE KEY 1
216
PUBLIC KEY 1 DELIVERED TO ACCOUNT MODULE
218
ACCOUNT MODULE SIGNS PUBLIC KEY 1 AND PSEUDONYM WITH SYSTEM'S PRIVATE KEY
220
DIGITAL CERTIFICATE 1 DELIVERED TO CLIENT
222
ACCOUNT MODULE GENERATES KEY PAIR 2
224
PRIVATE KEY 2 STORED IN ACCOUNT MODULE
226
PUBLIC KEY 2 AND PSEUDONYM SIGNED WITH SYSTEM'S PRIVATE KEY
228
STORE DIGITAL CERTIFICATE 2
230
END
232

FIG. 2

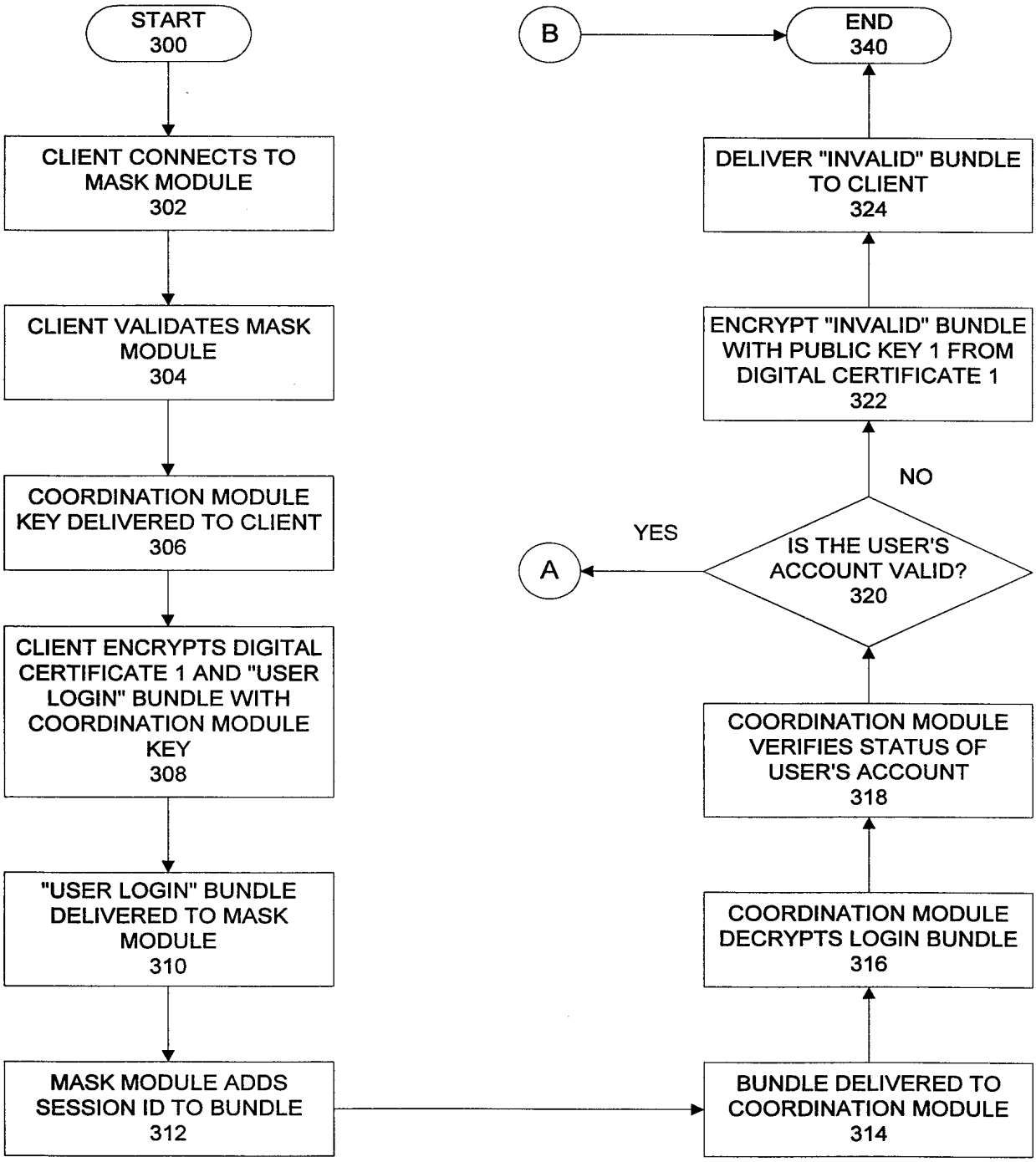

START
300
CLIENT CONNECTS TO MASK MODULE
302
CLIENT VALIDATES MASK MODULE
304
COORDINATION MODULE KEY DELIVERED TO CLIENT
306
CLIENT ENCRYPTS DIGITAL CERTIFICATE 1 AND "USER LOGIN" BUNDLE WITH COORDINATION MODULE KEY
308
"USER LOGIN" BUNDLE DELIVERED TO MASK MODULE
310
MASK MODULE ADDS SESSION ID TO BUNDLE
312
BUNDLE DELIVERED TO COORDINATION MODULE
314
COORDINATION MODULE DECRYPTS LOGIN BUNDLE
316
COORDINATION MODULE VERIFIES STATUS OF USER'S ACCOUNT
318
IS THE USER'S ACCOUNT VALID?
320
YES
A
NO
ENCRYPT "INVALID" BUNDLE WITH PUBLIC KEY 1 FROM DIGITAL CERTIFICATE 1
322
DELIVER "INVALID" BUNDLE TO CLIENT
324
B
END
340

FIG. 3A

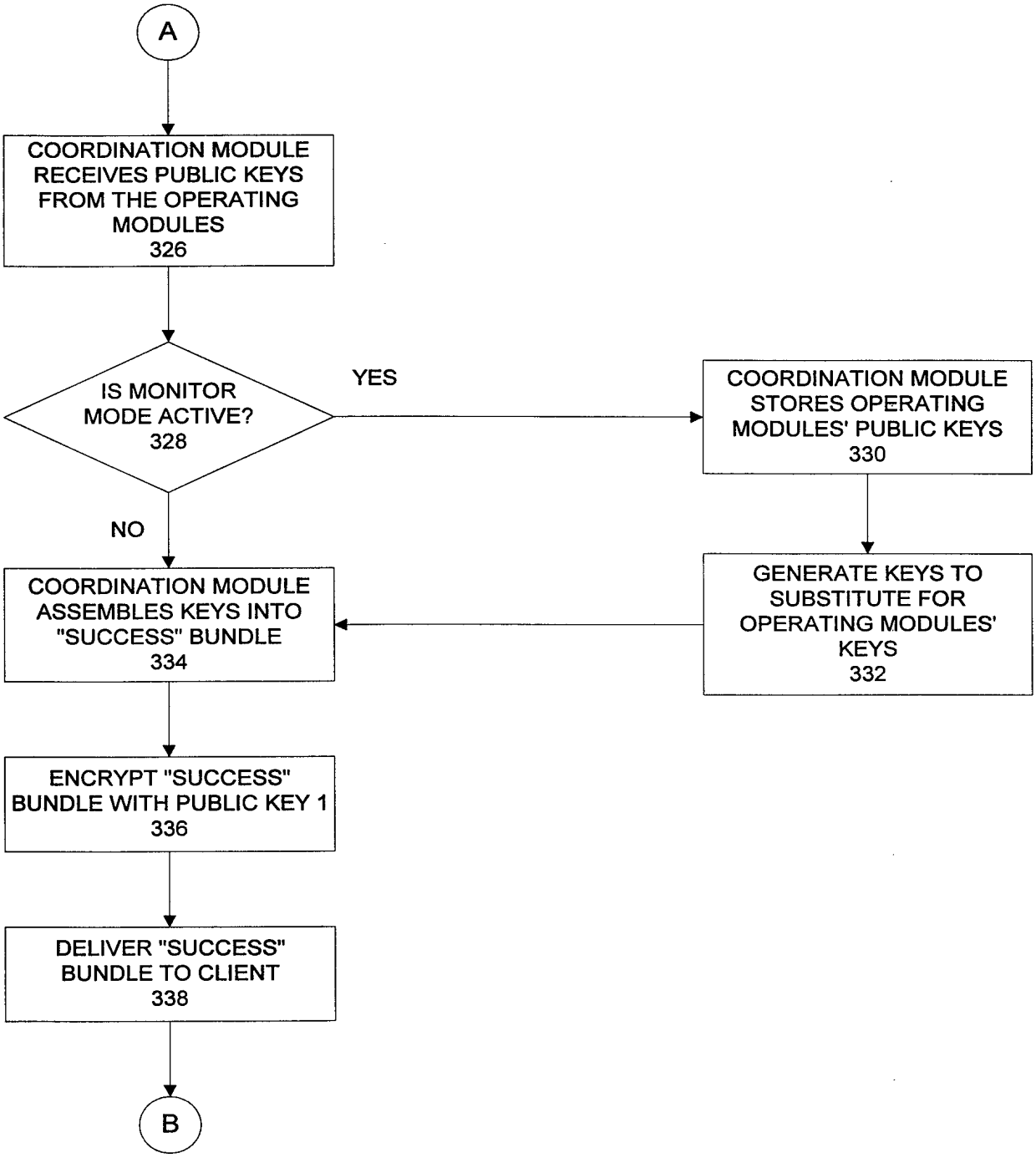

A
COORDINATION MODULE RECEIVES PUBLIC KEYS FROM THE OPERATING MODULES
326
IS MONITOR MODE ACTIVE?
328
YES
COORDINATION MODULE STORES OPERATING MODULES' PUBLIC KEYS
330
GENERATE KEYS TO SUBSTITUTE FOR OPERATING MODULES' KEYS
332
NO
COORDINATION MODULE ASSEMBLES KEYS INTO "SUCCESS" BUNDLE
334
ENCRYPT "SUCCESS" BUNDLE WITH PUBLIC KEY 1
336
DELIVER "SUCCESS" BUNDLE TO CLIENT
338
B

FIG. 3B

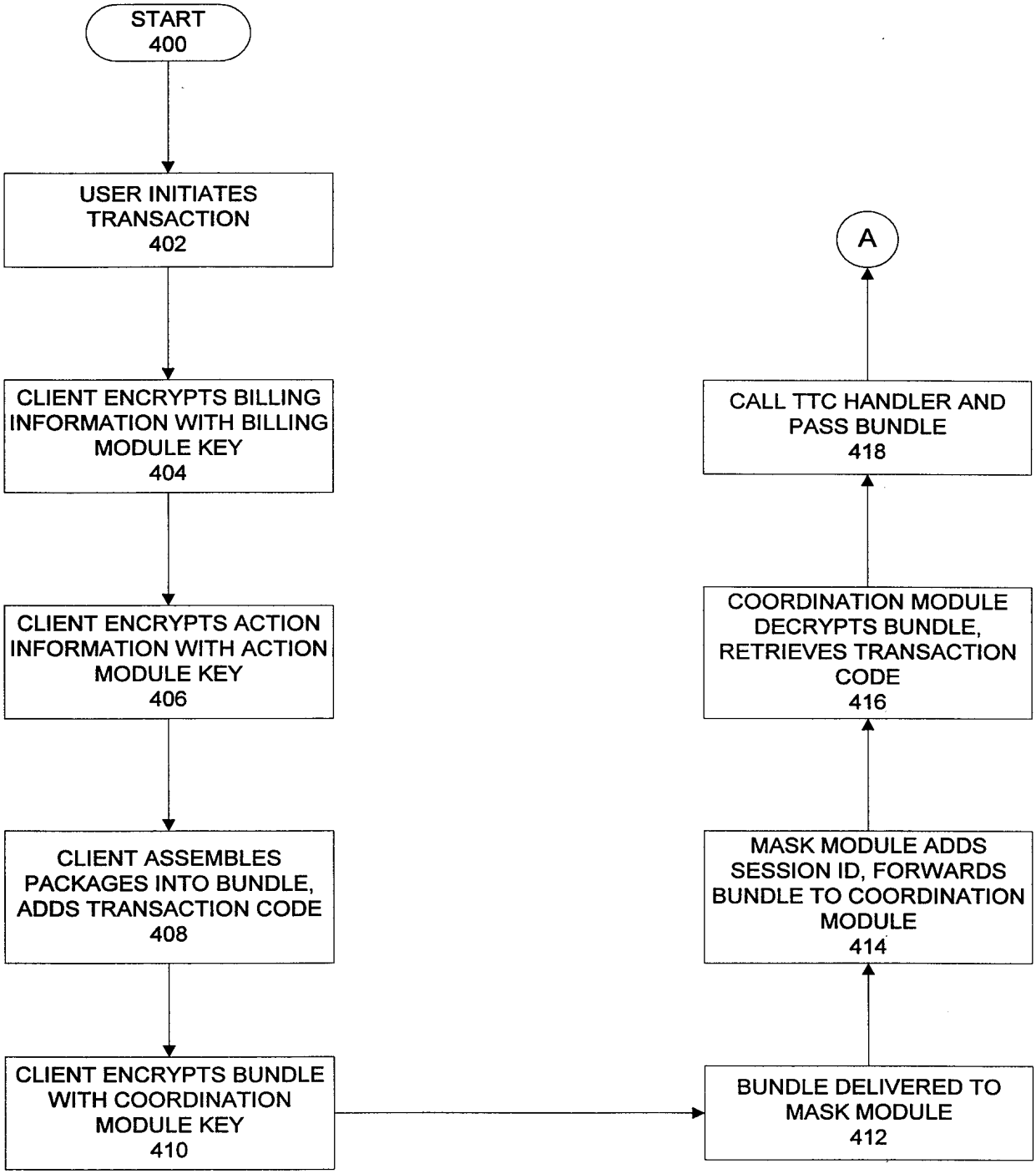

START
400
USER INITIATES TRANSACTION
402
CLIENT ENCRYPTS BILLING INFORMATION WITH BILLING MODULE KEY
404
CLIENT ENCRYPTS ACTION INFORMATION WITH ACTION MODULE KEY
406
CLIENT ASSEMBLES PACKAGES INTO BUNDLE, ADDS TRANSACTION CODE
408
CLIENT ENCRYPTS BUNDLE WITH COORDINATION MODULE KEY
410
BUNDLE DELIVERED TO MASK MODULE
412
MASK MODULE ADDS SESSION ID, FORWARDS BUNDLE TO COORDINATION MODULE
414
COORDINATION MODULE DECRYPTS BUNDLE, RETRIEVES TRANSACTION CODE
416
CALL TTC HANDLER AND PASS BUNDLE
418
A

FIG. 4A

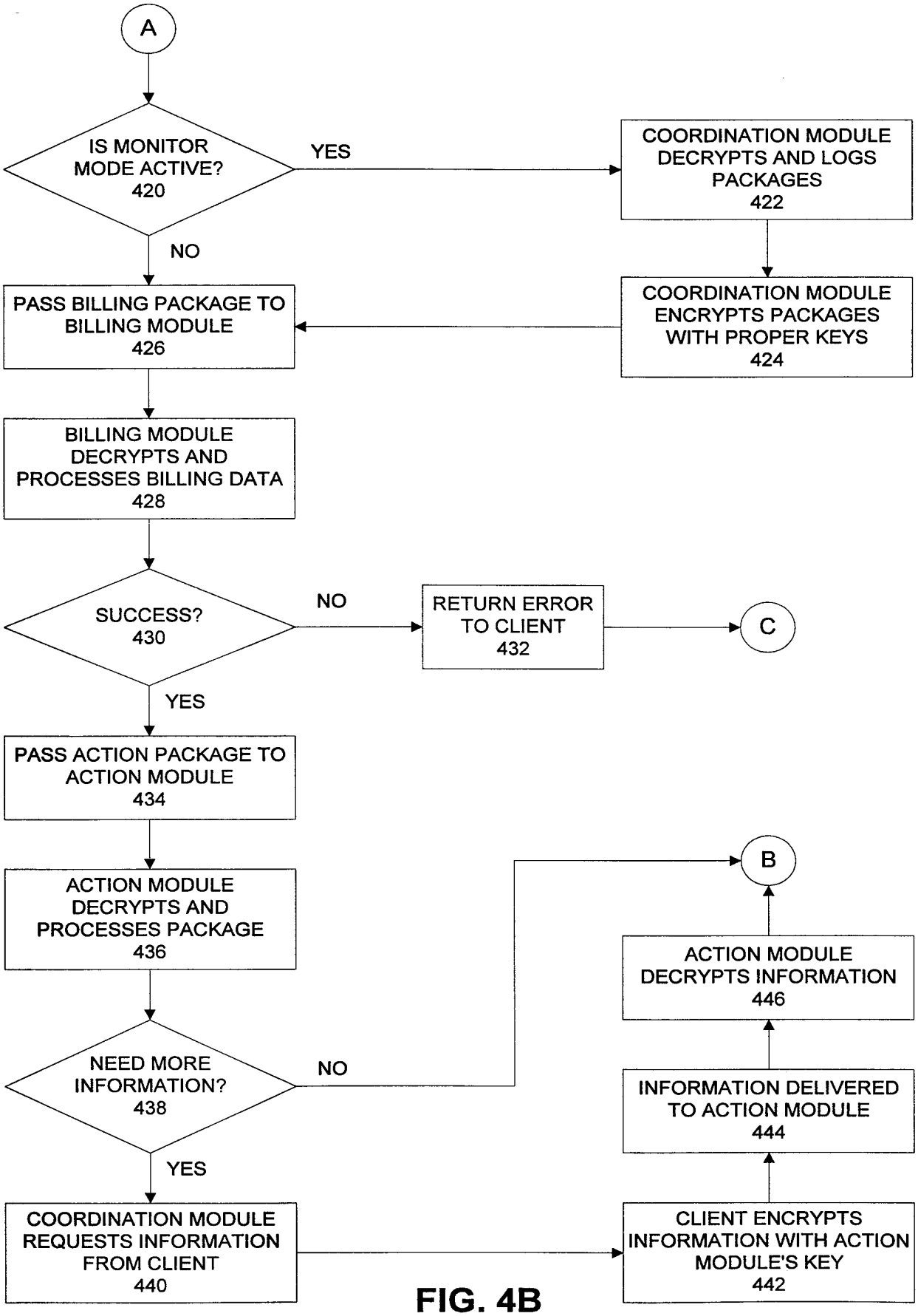

A
IS MONITOR MODE ACTIVE? 420
YES
COORDINATION MODULE DECRYPTS AND LOGS PACKAGES 422
NO
PASS BILLING PACKAGE TO BILLING MODULE 426
COORDINATION MODULE ENCRYPTS PACKAGES WITH PROPER KEYS 424
BILLING MODULE DECRYPTS AND PROCESSES BILLING DATA 428
SUCCESS? 430
NO
RETURN ERROR TO CLIENT 432
C
YES
PASS ACTION PACKAGE TO ACTION MODULE 434
ACTION MODULE DECRYPTS AND PROCESSES PACKAGE 436
B
ACTION MODULE DECRYPTS INFORMATION 446
NEED MORE INFORMATION? 438
NO
INFORMATION DELIVERED TO ACTION MODULE 444
YES
COORDINATION MODULE REQUESTS INFORMATION FROM CLIENT 440
CLIENT ENCRYPTS INFORMATION WITH ACTION MODULE'S KEY 442

FIG. 4B

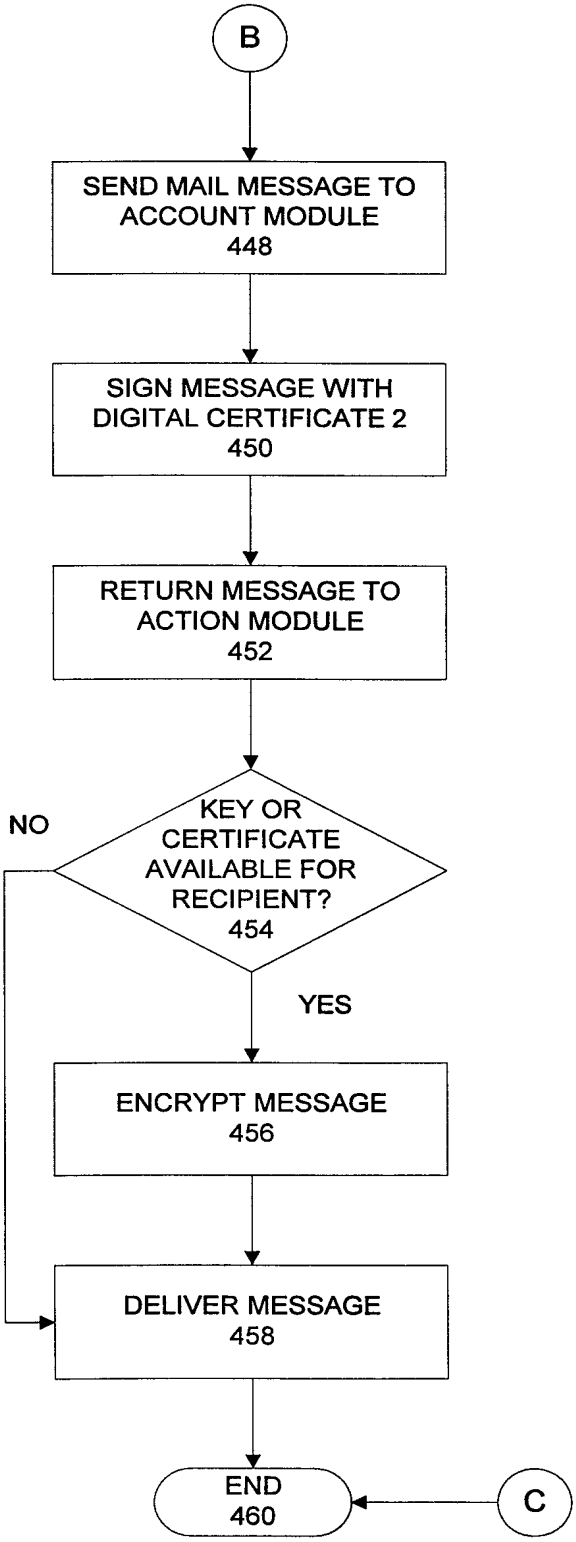

B
SEND MAIL MESSAGE TO ACCOUNT MODULE 448
SIGN MESSAGE WITH DIGITAL CERTIFICATE 2 450
RETURN MESSAGE TO ACTION MODULE 452
KEY OR CERTIFICATE AVAILABLE FOR RECIPIENT? 454
NO
YES
ENCRYPT MESSAGE 456
DELIVER MESSAGE 458
END 460
C

FIG. 4C

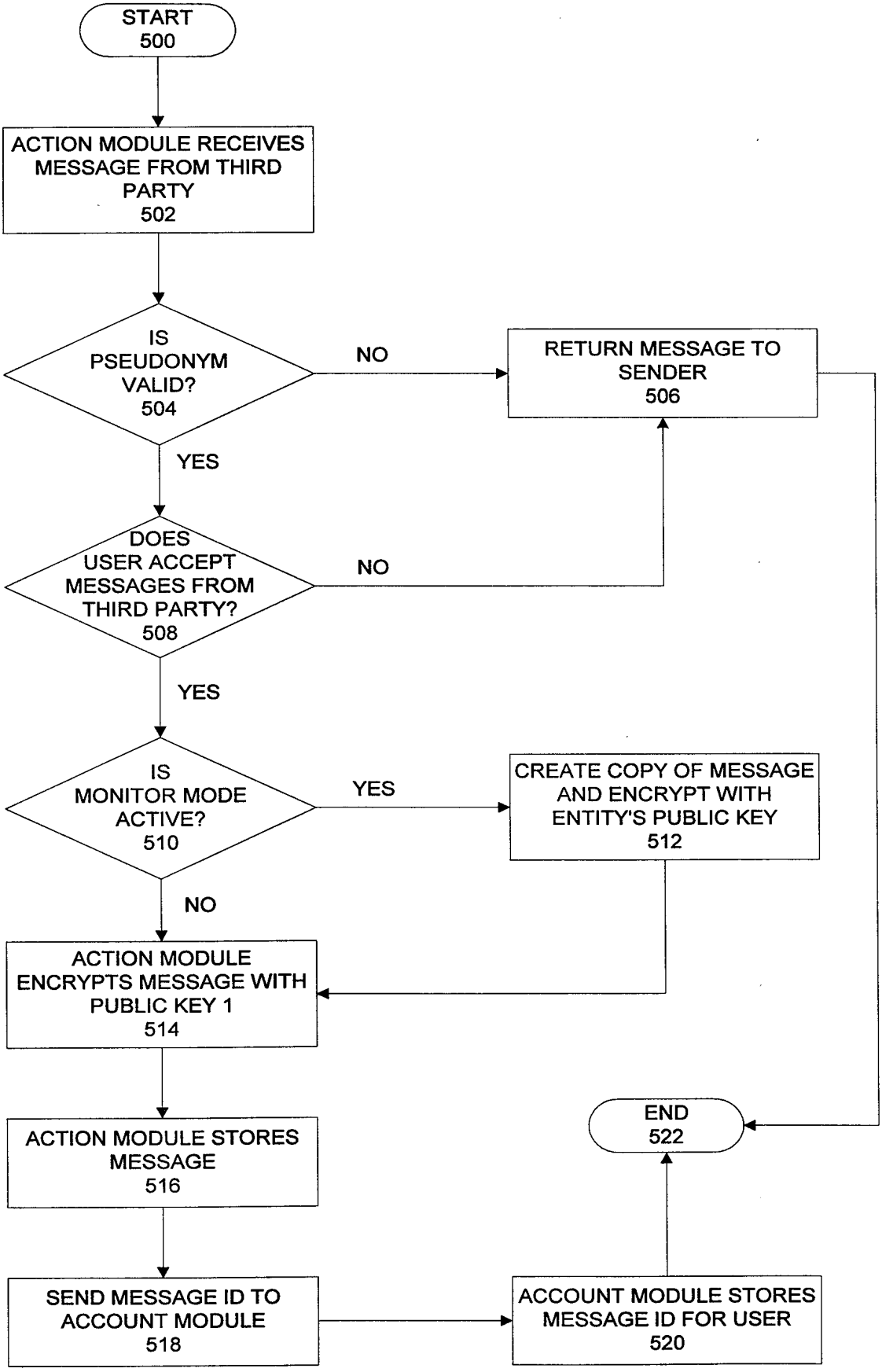

START
500
ACTION MODULE RECEIVES MESSAGE FROM THIRD PARTY
502
IS PSEUDONYM VALID?
504
NO
RETURN MESSAGE TO SENDER
506
YES
DOES USER ACCEPT MESSAGES FROM THIRD PARTY?
508
NO
YES
IS MONITOR MODE ACTIVE?
510
YES
CREATE COPY OF MESSAGE AND ENCRYPT WITH ENTITY'S PUBLIC KEY
512
NO
ACTION MODULE ENCRYPTS MESSAGE WITH PUBLIC KEY 1
514
ACTION MODULE STORES MESSAGE
516
END
522
SEND MESSAGE ID TO ACCOUNT MODULE
518
ACCOUNT MODULE STORES MESSAGE ID FOR USER
520

FIG. 5

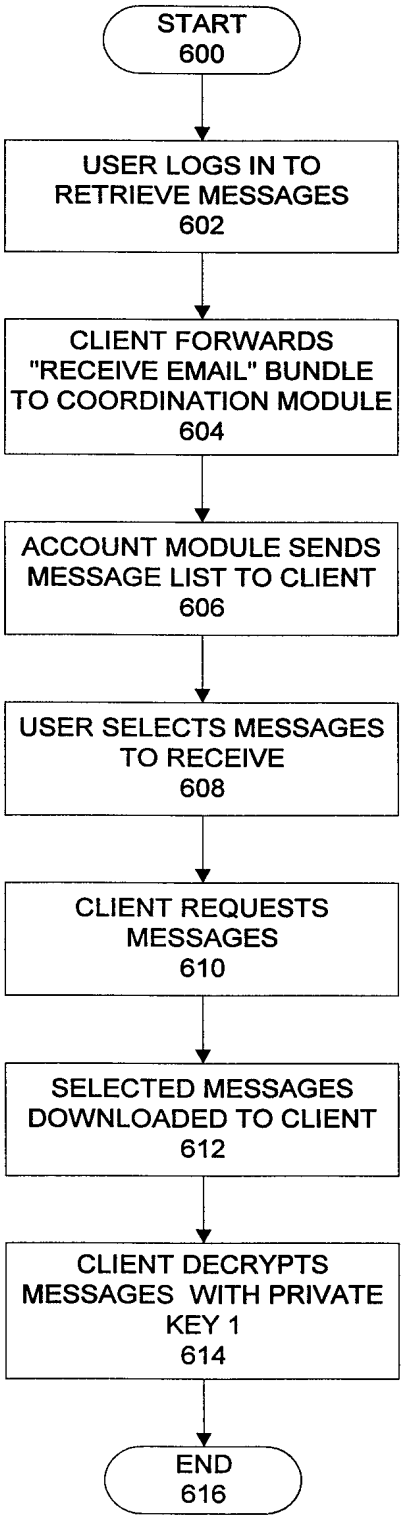

START
600
USER LOGS IN TO RETRIEVE MESSAGES
602
CLIENT FORWARDS "RECEIVE EMAIL" BUNDLE TO COORDINATION MODULE
604
ACCOUNT MODULE SENDS MESSAGE LIST TO CLIENT
606
USER SELECTS MESSAGES TO RECEIVE
608
CLIENT REQUESTS MESSAGES
610
SELECTED MESSAGES DOWNLOADED TO CLIENT
612
CLIENT DECRYPTS MESSAGES WITH PRIVATE KEY 1
614
END
616

FIG. 6